kaspersky

# Kaspersky Security Center (для Windows)

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 14.2.0.26967

kaspersky

Уважаемый пользователь!

Спасибо, что доверяете нам. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.



Дата публикации документа: 25.09.2023

Обозначение документа: 643.46856491.00069-10 90 02



https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

О "Лаборатории Касперского": (https://www.kaspersky.com/about/company)

kaspersky

# Содержание

kaspersky

# Об этом документе

Настоящий документ представляет собой подготовительные процедуры и руководство по эксплуатации программного изделия «Kaspersky Security Center» (для Windows) (далее также «Kaspersky Security Center», «программа»).

Подготовительные процедуры изложены в разделах "Подготовка к установке программы", "Установка программы", "Подготовка программы к работе" и "Процедура приемки" и содержат процедуры безопасной установки и первоначальной настройки программы, которые необходимы для получения безопасной (сертифицированной) конфигурации. В разделе "Требования" приведены минимально необходимые системные требования для безопасной установки программы.

Остальные разделы этого документа представляют собой руководство по эксплуатации. Руководство по эксплуатации содержит сведения о том, как осуществлять безопасное администрирование программы, а также инструкции и указания по безопасному использованию программы.

В документе также содержатся разделы с дополнительной информацией о программе.

Документ адресован техническим специалистам, в обязанности которых входит установка, эксплуатация и администрирование Kaspersky Security Center, а также поддержка организаций, использующих Kaspersky Security Center.

kaspersky

# Источники информации о программе

Указанные источники информации о программе (в частности, электронная онлайн-справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

**Страница Kaspersky Security Center на веб-сайте "Лаборатории Касперского"**

На странице Kaspersky Security Center (http://www.kaspersky.ru/security-center) вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

**Страница Kaspersky Security Center в Базе знаний**

*База знаний* – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На странице Kaspersky Security Center в Базе знаний вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Security Center и с другими программами "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. стр. 1489).

kaspersky

# Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде, а также список поддерживаемых программ "Лаборатории Касперского" и решений.

## В этом разделе



## Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление программой должны осуществляться в соответствии с эксплуатационной документацией.
2. Программа должна эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации программы необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ программы ко всем объектам информационной системы, которые необходимы программе для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость программы с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы программы со средствами антивирусной защиты других производителей в случае их совместного использования в информационной системе.
7. Должна быть обеспечена физическая защита элементов информационной системы, на которых установлена программа.
8. Должны быть обеспечены конфиденциальность и целостность первоначального соединения между Сервером администрирования и Агентами администрирования.
9. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
10. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
11. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
12. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
13. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
14. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.

15. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
16. Администратор должен установить в среде ИТ максимальное число попыток неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя с последующей блокировкой попыток аутентификации при превышении установленного значения.
17. Администратор должен задать метрику качества паролей, включающую требования к длине паролей, требования по запрещению использования определенных комбинаций символов, а также требования к категории используемых символов.

# Аппаратные и программные требования

**Сервер администрирования**

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: 10 ГБ. При использовании функциональности Системное администрирование объем свободного места на диске должен быть не менее 100 ГБ.

Для развертывания в облачных окружениях требования к Серверу администрирования и серверу базы данных такие же, как и к физическому Серверу администрирования (в зависимости от того, каким количеством устройств вы хотите управлять).

Программные требования:

- Microsoft® Data Access Components (MDAC) 2.8;
- Microsoft Windows® DAC 6.0;
- Microsoft Windows Installer 4.5.

Поддерживаются следующие операционные системы:

- Windows Server 2008 R2 Standard Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;

- Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Windows Server 2016 Standard (LTSB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2019 64-разрядная.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x.

Поддерживаются следующие серверы баз данных (могут быть установлены на другом устройстве):

- Microsoft SQL Server 2012 Express 64-разрядная;
- Microsoft SQL Server 2014 Express 64-разрядная;
- Microsoft SQL Server 2016 Express 64-разрядная;
- Microsoft SQL Server 2017 Express 64-разрядная;
- Microsoft SQL Server 2019 Express 64-разрядная;
- Microsoft SQL Server 2014 (все редакции) 64-разрядная;
- Microsoft SQL Server 2016 (все редакции) 64-разрядная;
- Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;

- Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
- Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия (см. стр. 164));
- Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия (см. стр. 164));
- Microsoft Azure SQL Database;
- Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;
- MySQL 5.7 Community 32-разрядная/64-разрядная;
- MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная;
- MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная;
- MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
- PostgreSQL 13.x 64-разрядная;
- PostgreSQL 14.x 64-разрядная;
- Postgres Pro Standard 13.x 64-разрядная;
- Postgres Pro Standard 14.x 64-разрядная;
- Postgres Pro Certified 14.x 64-разрядная.

Рекомендуется использовать версию MariaDB 10.3.22; если вы используете более раннюю версию, задача обновления Windows может выполнятся более одного дня.

SIEM-системы и другие системы управления информацией:

- HP (Micro Focus) ArcSight ESM 7.0;
- IBM QRadar 7.3;
- Splunk 7.1.

**Kaspersky Security Center Web Console**

**Сервер Kaspersky Security Center 14.2 Web Console**

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2,5 ГГц.
- ОЗУ: 8 ГБ.
- Объем свободного места на диске: 40 ГБ.

Поддерживаются следующие операционные системы:

- Microsoft Windows (только 64-разрядные версии):
  - Windows Server 2012 Server Core;
  - Windows Server 2012 Datacenter;
  - Windows Server 2012 Essentials;
  - Windows Server 2012 Foundation;
  - Windows Server 2012 Standard;
  - Windows Server 2012 R2 Server Core;
  - Windows Server 2012 R2 Datacenter;
  - Windows Server 2012 R2 Essentials;
  - Windows Server 2012 R2 Foundation;
  - Windows Server 2012 R2 Standard;
  - Windows Server 2016 Datacenter (LTSB);
  - Windows Server 2016 Standard (LTSB);
  - Windows Server 2016 (вариант установки Server Core) (LTSB);
  - Windows Server 2019 Standard;
  - Windows Server 2019 Datacenter;
  - Windows Server 2019 Core;
  - Windows Server 2022 Standard;
  - Windows Server 2022 Datacenter;
  - Windows Server 2022 Core;
  - Windows Storage Server 2012;
  - Windows Storage Server 2012 R2;
  - Windows Storage Server 2016;
  - Windows Storage Server 2019;
- Linux (только 64-разрядные версии):
  - Debian GNU/Linux 9.x (Stretch);
  - Debian GNU/Linux 10.x (Buster);
  - Debian GNU/Linux 11.x (Bullseye);
  - Ubuntu Server 18.04 LTS (Bionic Beaver);
  - Ubuntu Server 20.04 LTS (Focal Fossa);
  - Ubuntu Server 22.04 LTS (Jammy Jellyfish);
  - CentOS 7.x;
  - Red Hat Enterprise Linux Server 7.x;
  - Red Hat Enterprise Linux Server 8.x;

- Red Hat Enterprise Linux Server 9.x;
- SUSE Linux Enterprise Server 12 (все пакеты обновлений);
- SUSE Linux Enterprise Server 15 (все пакеты обновлений).
- Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим);
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды и мандатный режим);
- Astra Linux Common Edition 2.12;
- ALT Server 9.2;
- ALT Server 10;
- Альт 8 СП Сервер (ЛКНВ.11100-01);
- Альт 8 СП Сервер (ЛКНВ.11100-02);
- Альт 8 СП Сервер (ЛКНВ.11100-03);
- Oracle Linux 7;
- Oracle Linux 8;
- Oracle Linux 9;
- РЕД ОС 7.3 Сервер;
- РЕД ОС 7.3 Сертифицированная редакция.

Виртуальная машина на основе Kernel поддерживается следующими операционными системами, рекомендованными для виртуальных сред Kaspersky Security Center:

- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- ALT Server 10 64-разрядная;
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды и мандатный режим);
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

**Клиентские устройства**

Клиентскому устройству для работы с Kaspersky Security Center 14.2 Web Console требуется только браузер.

Требования к аппаратному и программному обеспечению устройства соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center 14.2 Web Console.

Браузеры:

- Mozilla Firefox Extended Support Release 91.8.0 или более поздняя версия (релиз 91.8.0 выпущен 5 апреля 2022);
- Google Chrome 100.0.4896.88 или более поздняя версия (официальная сборка);
- Microsoft Edge 100 или более поздняя версия;

- Safari 15 для macOS.

**Сервер мобильных устройств iOS Mobile Device Management (iOS MDM)**

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 2 ГБ.
- Объем свободного места на диске: 2 ГБ.

Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования).

**Сервер мобильных устройств Exchange ActiveSync**

Программные и аппаратные требования для Сервера мобильных устройств Exchange ActiveSync полностью включены в требования для сервера Microsoft Exchange Server.

Поддерживается работа с Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 и Microsoft Exchange Server 2013.

**Консоль администрирования**

Аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- Оперативная память: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Программные требования:

- Операционная система Microsoft Windows (версия поддерживаемой операционной системы определяется требованиями Сервера администрирования), исключая следующие операционные системы:
  - Windows Server 2012 Server Core 64-разрядная;
  - Windows Server 2012 R2 Server Core 64-разрядная;
  - Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
  - Windows Server 2019 Core 64-разрядная;
  - Windows Server 2022 Core 64-разрядная;
- Microsoft Management Console 2.0;
- Microsoft Windows Installer 4.5;
- Microsoft Internet Explorer 10.0 работает на:
  - Microsoft Windows Server 2008 R2 Service Pack 1;
  - Microsoft Windows Server 2012;
  - Microsoft Windows Server 2012 R2;
  - Microsoft Windows 7 Service Pack 1;

  - Microsoft Windows 8;
  - Microsoft Windows 8.1;
  - Microsoft Windows 10;
- Microsoft Internet Explorer 11.0 работает на:
  - Microsoft Windows Server 2012 R2;
  - Microsoft Windows Server 2012 R2 Service Pack 1;
  - Microsoft Windows Server 2016;
  - Microsoft Windows Server 2019;
  - Microsoft Windows 7 Service Pack 1;
  - Microsoft Windows 8.1;
  - Microsoft Windows 10;
- Microsoft Edge, запущенный на Microsoft Windows 10.

**Агент администрирования**

Минимальные аппаратные требования:

- Процессор с частотой 1 ГГц или выше. При работе с 64-разрядной операционной системой минимальная частота процессора – 1.4 ГГц.
- ОЗУ: 512 МБ.
- Объем свободного места на диске: 1 ГБ.

Требования к программному обеспечению для устройств с операционной системой Linux: должен быть установлен интерпретатор языка Perl версии 5.10 или выше.

Поддерживаются следующие операционные системы:

- Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная;
- Microsoft Windows Embedded POSReady 7 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 7 Standard Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Standard 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Update 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная;

- Microsoft Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная;
- Microsoft Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1902 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS3 (Fall Creators Update, v1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home RS5 (октябрь 2018) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (октябрь 2018) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (октябрь 2018) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (октябрь 2018) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (октябрь 2018) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 11 22H2;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium with Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная (поддерживается Агентом администрирования версии 10.5);
- Microsoft Windows XP Professional Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;
- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;

- Windows MultiPoint Server 2011 Standard / Premium 64-разрядная;
- Windows MultiPoint Server 2012 Standard / Premium 64-разрядная;
- Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 2 (все редакции) 32-разрядная/64-разрядная;
- Windows Server 2008 R2 Datacenter Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Enterprise Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Foundation Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Core Mode Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Standard Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 Datacenter 64-разрядная;
- Windows Server 2012 Essentials 64-разрядная;
- Windows Server 2012 Foundation 64-разрядная;
- Windows Server 2012 Standard 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2012 R2 Datacenter 64-разрядная;
- Windows Server 2012 R2 Essentials 64-разрядная;
- Windows Server 2012 R2 Foundation 64-разрядная;
- Windows Server 2012 R2 Standard 64-разрядная;
- Windows Server 2016 Datacenter (LTSB) 64-разрядная;
- Windows Server 2016 Standard (LTSB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Windows Server 2019 Standard 64-разрядная;
- Windows Server 2019 Datacenter 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Standard 64-разрядная;
- Windows Server 2022 Datacenter 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2012 64-разрядная;
- Windows Storage Server 2012 R2 64-разрядная;
- Windows Storage Server 2016 64-разрядная;
- Windows Storage Server 2019 64-разрядная;
- Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная;
- Debian GNU / Linux 10.x (Buster) 32-разрядная/64-разрядная;

- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) ARM 64-разрядная;
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-разрядная/64-разрядная;
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-разрядная/64-разрядная;
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная;
- CentOS 7.x 64-разрядная;
- CentOS 7.x ARM 64-разрядная;
- Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная;
- Red Hat Enterprise Linux Server 7.x 64-разрядная;
- Red Hat Enterprise Linux Server 8.x 64-разрядная;
- Red Hat Enterprise Linux Server 9.x 64-разрядная;
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;
- SUSE Linux Enterprise Desktop 15 (все пакеты обновлений) 64-разрядная;
- SUSE Linux Enterprise Desktop 15 Service Pack 3 ARM 64-разрядная;
- openSUSE 15 64-разрядная;
- EulerOS 2.0 SP8 ARM;
- Pardus OS 19.1 64-разрядная;
- Astra Linux Common Edition 2.12 64-разрядная;
- Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды (см. стр. 209) и мандатный режим) 64-разрядная;
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Special Edition 4.7 ARM;
- Альт Сервер 9,2 64-разрядная;
- ALT Server 10 64-разрядная;
- Альт Рабочая станция 9,2 32-разрядная/64-разрядная;
- Альт Рабочая станция 10 32-разрядная/64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;
- Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;
- Альт 8 СП Рабочая станция (LKNV.11100-01) 32-разрядная/64-разрядная;
- Альт 8 СП Рабочая станция (LKNV.11100-02) 32-разрядная/64-разрядная;
- Альт 8 СП Рабочая станция (LKNV.11100-03) 32-разрядная/64-разрядная;

- Mageia 4 32-разрядная.
- Oracle Linux 7 64-разрядная;
- Oracle Linux 8 64-разрядная;
- Oracle Linux 9 64-разрядная;
- Linux Mint 19.x 32-разрядная;
- Linux Mint 20.x 64-разрядная;
- AlterOS 7.5 или более поздняя версия 64-разрядная;
- GosLinux IC6 64-разрядная;
- РЕД ОС 7.3 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная;
- РОСА "ХРОМ" 12 64-разрядная;
- Лотос (версия ядра Linux 4.19.50, DE: MATE 8.3) 64-разрядная.
- macOS Sierra (10.12);
- macOS High Sierra (10.13);
- macOS Mojave (10.14);
- macOS Catalina (10.15);
- macOS Big Sur (11.x);
- macOS Monterey (12.x).

Для Агента администрирования поддерживается архитектура Apple Silicon (M1), также, как и Intel.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядная;
- Microsoft Hyper-V Server 2012 R2 64-разрядная;
- Microsoft Hyper-V Server 2016 64-разрядная;
- Microsoft Hyper-V Server 2019 64-разрядная;
- Microsoft Hyper-V Server 2022 64-разрядная;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Виртуальная машина на основе Kernel поддерживается следующими операционными системами, рекомендованными для виртуальных сред Kaspersky Security Center:
  - Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

- ALT Server 10 64-разрядная;
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды (см. стр. 209) и мандатный режим) 64-разрядная;
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- РЕД ОС 7.3 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

На устройствах под управлением Windows 10 версии RS4 или RS5 Kaspersky Security Center может не обнаруживать некоторые уязвимости в папках, в которых включен учет регистра.
Перед установкой Агента администрирования на устройства под управлением Windows 7, Windows Server 2008 или Windows Small Business Server 2011 Premium убедитесь, что у вас установлено обновление для Windows 7 (KB3063858).
В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно (см. стр. 178).
Вы можете установить или обновить Агент администрирования для Windows XP только в Microsoft Windows XP.
Рекомендуется устанавливать ту же версию Агента администрирования для Linux, что и Kaspersky Security Center.
Агент администрирования для macOS поставляется вместе с программой безопасности "Лаборатории Касперского" для этой операционной системы.

### См. также:

Основной сценарий установки.....92

## Неподдерживаемые операционные системы и платформы

**Сервер администрирования**

Сервер администрирования несовместим со следующими операционными системами:

- Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная;
- Microsoft Windows Embedded POSReady 7 32-разрядная/64-разрядная;
- Microsoft Windows Embedded Standard 7 Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Standard 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Update 32-разрядная/64-разрядная;

- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная;
- Microsoft Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1902 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;

- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS3 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS3 32-разрядная;
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS4 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS4 32-разрядная;
- Microsoft Windows 10 Home RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS5 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS5 32-разрядная;
- Microsoft Windows 10 Home 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;

- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 11 22H2;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 (Core) 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium with Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;

- Microsoft Windows Vista Business Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Professional Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Home Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная;
- Microsoft Essential Business Server 2008 Standard 64-разрядная;
- Microsoft Essential Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2003 Standard Service Pack 1 32-разрядная;
- Windows Small Business Server 2003 Premium Service Pack 1 32-разрядная;
- Windows Small Business Server 2008 Standard 64-разрядная;
- Windows Small Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;
- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Home Server 2011 64-разрядная;
- Windows MultiPoint Server 2010 Standard 64-разрядная;
- Windows MultiPoint Server 2010 Premium 64-разрядная;
- Windows MultiPoint Server 2011 Standard 64-разрядная;
- Windows MultiPoint Server 2011 Premium 64-разрядная;
- Windows MultiPoint Server 2012 Standard 64-разрядная;
- Windows MultiPoint Server 2012 Premium 64-разрядная;
- Microsoft Windows 2000 Server 32-разрядная;
- Windows Server 2003 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 1 Server Core 32-разрядная/64-разрядная;

- Windows Server 2008 Standard Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Standard 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 2 (все редакции) 32-разрядная/64-разрядная;
- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter Service Pack 1 или более поздняя версия 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Core Mode Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2016 (вариант установки Nano) (CBB) 64-разрядная;
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Nano RS3 (1709) (CBB) 64-разрядная;
- Windows Storage Server 2008 32-разрядная/64-разрядная;
- Windows Storage Server 2008 Service Pack 2 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная.

Сервер баз данных:

- PostgreSQL 15 64-разрядная;
- PostgreSQL Pangolin 64-разрядная;
- Microsoft SQL Server 2005 Express 32-разрядная;
- Microsoft SQL Server 2005 (все редакции) 32-разрядная/64-разрядная;
- Microsoft SQL Server 2008 Express 32-разрядная;
- Microsoft SQL Server 2008 (все редакции) 32-разрядная/64-разрядная;
- Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2008 R2 Service Pack 2 (все редакции) 64-разрядная;
- Microsoft SQL Server 2012 (все редакции за исключением Express) 32-разрядная/64-разрядная;
- MySQL 5.0 32-разрядная/64-разрядная;
- MySQL Enterprise 5.0 32-разрядная/64-разрядная;
- MySQL Standard Edition 5.5 32-разрядная/64-разрядная;

- MySQL Enterprise Edition 5.5 32-разрядная/64-разрядная;
- MySQL Standard Edition 5.6 32-разрядная/64-разрядная;
- MySQL Enterprise Edition 5.6 32-разрядная/64-разрядная;
- MySQL Standard Edition 5.7 32-разрядная/64-разрядная;
- MySQL Enterprise Edition 5.7 32-разрядная/64-разрядная;
- MySQL 5.6 Community 32-разрядная/64-разрядная;
- MariaDB Galera Cluster 10.4 32-разрядная/64-разрядная.

Следующие платформы виртуализации не поддерживаются:

- VMware vSphere 4.1;
- VMware vSphere 5.0;
- VMware vSphere 5.1;
- VMware vSphere 5.5;
- VMware vSphere 7.0;
- VMware vSphere 6.5;
- VMware Workstation 9.x;
- VMware Workstation 10.x;
- VMware Workstation 11.x;
- VMware Workstation 12.x Pro;
- VMware Workstation Pro 14;
- VMware Workstation Pro 15;
- Microsoft Hyper-V Server 2008 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 64-разрядная;
- Microsoft Virtual PC 2007 (6.0.156.0) 32-разрядная/64-разрядная;
- Citrix XenServer 5.6;
- Citrix XenServer 6.0;
- Citrix XenServer 6.1;
- Citrix XenServer 6.2;
- Citrix XenServer 6.5.
- Citrix XenServer 7.
- Parallels Desktop 7;
- Parallels Desktop 11;
- Parallels Desktop 14;
- Parallels Desktop 16;
- Oracle VM VirtualBox 4.0.4-70112 (только гостевой вход Windows);

- Oracle VM VirtualBox 5.x.

**Kaspersky Security Center 14.2 Web Console**

**Сервер Kaspersky Security Center 14.2 Web Console**

Сервер Kaspersky Security Center 14.2 Web Console несовместим со следующими операционными системами:

- Microsoft Windows:
  - Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная;
  - Microsoft Windows Embedded POSReady 7 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded Standard 7 Service Pack 1 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8 Standard 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8 Industry Pro 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8 Industry Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8.1 Industry Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows Embedded 8.1 Industry Update 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/ARM;
  - Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/ARM;
  - Microsoft Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная;
  - Microsoft Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise версия 1902 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная;
  - Microsoft Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Home (Threshold 1, 1507) 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Pro (Threshold 1, 1507) 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Education (Threshold 1, 1507) 32-разрядная/64-разрядная;
  - Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-разрядная;

- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS3 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS3 32-разрядная;
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS4 32-разрядная;

- Microsoft Windows 10 Mobile Enterprise RS4 32-разрядная;
- Microsoft Windows 10 Home RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (октябрь 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS5 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS5 32-разрядная;
- Microsoft Windows 10 Home 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update);
- Microsoft Windows 10 Pro 20H2 (October 2020 Update);
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update);
- Microsoft Windows 10 Education 20H2 (October 2020 Update);
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 11 22H2;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8 (Core) 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium with Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Professional Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Home Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная;
- Microsoft Essential Business Server 2008 Standard 64-разрядная;
- Microsoft Essential Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2003 Standard Service Pack 1 32-разрядная;
- Windows Small Business Server 2003 Premium Service Pack 1 32-разрядная;
- Windows Small Business Server 2008 Standard 64-разрядная;
- Windows Small Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;

- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Home Server 2011 64-разрядная;
- Windows MultiPoint Server 2010 Standard 64-разрядная;
- Windows MultiPoint Server 2010 Premium 64-разрядная;
- Windows MultiPoint Server 2011 Standard 64-разрядная;
- Windows MultiPoint Server 2011 Premium 64-разрядная;
- Windows MultiPoint Server 2012 Standard 64-разрядная;
- Windows MultiPoint Server 2012 Premium 64-разрядная;
- Microsoft Windows 2000 Server 32-разрядная;
- Windows Server 2003 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 1 Server Core 32-разрядная/64-разрядная;
- Windows Server 2008 Standard Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Standard 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 2 (все редакции) 32-разрядная/64-разрядная;
- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter Service Pack 1 или более поздняя версия 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Core Mode Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2008 R2 Standard Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
- Windows Server 2016 (вариант установки Nano) (CBB) 64-разрядная;

- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Nano RS3 (1709) (CBB) 64-разрядная;
- Windows Storage Server 2008 32-разрядная/64-разрядная;
- Windows Storage Server 2008 Service Pack 2 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;

- Linux:
  - Debian GNU/Linux 7.x (до 7.8) 32-разрядная/64-разрядная;
  - Debian GNU/Linux 8.x (Jessie) 32-разрядная/64-разрядная;
  - Ubuntu Server 14.04 LTS (Trusty Tahr) 32-разрядная/64-разрядная;
  - Ubuntu Server 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная;
  - Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-разрядная/64-разрядная;
  - Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная;
  - Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-разрядная/64-разрядная;
  - Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-разрядная/64-разрядная;
  - CentOS 6.x (до 6.6) 64-разрядная;
  - CentOS 7.x ARM 64-разрядная;
  - CentOS 8.x 64-разрядная;
  - Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная;
  - SUSE Linux Enterprise Desktop 12 (все пакеты обновлений) 64-разрядная;
  - SUSE Linux Enterprise Desktop 15 (все пакеты обновлений) 64-разрядная;
  - SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-разрядная;
  - openSUSE 15 64-разрядная.
  - EulerOS 2.0 SP8 ARM;
  - Pardus OS 19.1 64-разрядная;
  - Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
  - Astra Linux Special Edition 4.7 ARM;
  - Альт Рабочая станция 10 32-разрядная/64-разрядная;
  - Альт 8 СП Рабочая станция (LKNV.11100-01) 32-разрядная/64-разрядная;
  - Альт 8 СП Рабочая станция (LKNV.11100-02) 32-разрядная/64-разрядная;
  - Альт 8 СП Рабочая станция (LKNV.11100-03) 32-разрядная/64-разрядная;
  - Mageia 4 32-разрядная;
  - Linux Mint 19.x 32-разрядная;

- Linux Mint 20.x 64-разрядная;
- AlterOS 7.5 или более поздняя версия 64-разрядная;
- РЕД ОС 7.3 64-разрядная;
- GosLinux IC6 64-разрядная;
- ROSA Enterprise Linux Server 7.3 64-разрядная;
- ROSA Linux Enterprise Desktop 7.3 64-разрядная;
- РОСА "КОБАЛЬТ" Рабочая станция 7.3 64-разрядная;
- РОСА "КОБАЛЬТ" Сервер 7.3 64-разрядная;
- РОСА "КОБАЛЬТ" 7.9 64-разрядная;
- РОСА "ХРОМ" 12 64-разрядная;
- Лотос (версия ядра Linux 4.19.50, DE: MATE 8.3) 64-разрядная.

**Консоль администрирования**

Консоль администрирования несовместима со следующими операционными системами:

- Microsoft Windows Embedded POSReady 2009 с последним Service Pack 32-разрядная;
- Microsoft Windows Embedded POSReady 7 32-разрядная/64-разрядная;
- Microsoft Windows Embedded Standard 7 Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Standard 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8.1 Industry Update 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/ARM;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1703 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1709 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1803 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1809 32-разрядная/64-разрядная;
- Microsoft Windows 10 20H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 21H2 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1902 32-разрядная/64-разрядная;

- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная;
- Microsoft Windows 10 IoT Enterprise версия 1607 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Home RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS3 (Fall Creators Update, 1709) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS3 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS3 32-разрядная;
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;

- Microsoft Windows 10 Pro Mobile Enterprise RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS4 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS4 32-разрядная;
- Microsoft Windows 10 Home RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций RS5 (октябрь 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS5 (October 2018 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS5 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS5 32-разрядная;
- Microsoft Windows 10 Home 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 2020 Update);
- Microsoft Windows 10 Pro 20H2 (October 2020 Update);
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update);
- Microsoft Windows 10 Education 20H2 (October 2020 Update);
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 64-разрядная;
- Microsoft Windows 11 22H2;
- Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
- Microsoft Windows 8 (Core) 32-разрядная/64-разрядная;
- Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium with Professional Service Pack 1 или более поздняя версия 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Professional Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Home Service Pack 3 32-разрядная;
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная;
- Microsoft Essential Business Server 2008 Standard 64-разрядная;
- Microsoft Essential Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2003 Standard Service Pack 1 32-разрядная;

- Windows Small Business Server 2003 Premium Service Pack 1 32-разрядная;
- Windows Small Business Server 2008 Standard 64-разрядная;
- Windows Small Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2011 Essentials 64-разрядная;
- Windows Small Business Server 2011 Premium Add-on 64-разрядная;
- Windows Small Business Server 2011 Standard 64-разрядная;
- Microsoft Windows Home Server 2011 64-разрядная;
- Windows MultiPoint Server 2010 Standard 64-разрядная;
- Windows MultiPoint Server 2010 Premium 64-разрядная;
- Windows MultiPoint Server 2011 Standard 64-разрядная;
- Windows MultiPoint Server 2011 Premium 64-разрядная;
- Windows MultiPoint Server 2012 Standard 64-разрядная;
- Windows MultiPoint Server 2012 Premium 64-разрядная;
- Microsoft Windows 2000 Server 32-разрядная;
- Windows Server 2003 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 1 Server Core 32-разрядная/64-разрядная;
- Windows Server 2008 Standard Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Standard 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 2 (все редакции) 32-разрядная/64-разрядная;
- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Windows Server 2008 R2 Datacenter Service Pack 1 или более поздняя версия 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Enterprise Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Foundation Service Pack 1 или более поздняя версия 64-разрядная;
- Windows Server 2008 R2 Core Mode Service Pack 1 или более поздняя версия 64-разрядная;

- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2012 Server Core 64-разрядная;
- Windows Server 2012 R2 Server Core 64-разрядная;
- Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
- Windows Server 2016 (вариант установки Nano) (CBB) 64-разрядная;
- Windows Server 2016 Server Datacenter RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 Server Standard RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Server Core RS3 (1709) (LTSB/CBB) 64-разрядная;
- Windows Server 2016 (вариант установки Nano RS3 (1709) (CBB) 64-разрядная;
- Windows Server 2019 Core 64-разрядная;
- Windows Server 2022 Core 64-разрядная;
- Windows Storage Server 2008 32-разрядная/64-разрядная;
- Windows Storage Server 2008 Service Pack 2 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная.

**Агент администрирования**

Следующие операционные системы не поддерживаются:

- Microsoft Windows Embedded 8 Industry Pro 32-разрядная/64-разрядная;
- Microsoft Windows Embedded 8 Industry Enterprise 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education (Threshold 1, 1507) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise (Threshold 1, 1507) 32-разрядная;
- Microsoft Windows 10 Home Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education Threshold 2 (November 2015 Update, 1511) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise Threshold 2 (November 2015 Update, 1511) 32-разрядная;
- Microsoft Windows 10 Home RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS1 (Anniversary Update, 1607) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS1 (Anniversary Update, 1607) 32-разрядная;

- Microsoft Windows 10 Mobile Enterprise RS1 (Anniversary Update, 1607) 32-разрядная;
- Microsoft Windows 10 Home RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Pro RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Enterprise RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Education RS2 (Creators Update, 1703) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Mobile RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS2 (Creators Update, 1703) 32-разрядная;
- Microsoft Windows 10 Mobile RS3 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS3 32-разрядная;
- Microsoft Windows 10 Mobile RS4 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS4 32-разрядная;
- Microsoft Windows 10 Mobile RS5 32-разрядная;
- Microsoft Windows 10 Mobile Enterprise RS5 32-разрядная;
- Microsoft Windows 8 (Core) 32-разрядная/64-разрядная;
- Microsoft Windows 7 Professional 32-разрядная/64-разрядная;
- Microsoft Windows 7 Enterprise/Ultimate 32-разрядная/64-разрядная;
- Microsoft Windows 7 Home Basic/Premium 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 1 32-разрядная/64-разрядная;
- Microsoft Windows Vista Business Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows Vista Ultimate Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная;
- Microsoft Windows XP Home Service Pack 3 32-разрядная;
- Microsoft Essential Business Server 2008 Standard 64-разрядная;
- Microsoft Essential Business Server 2008 Premium 64-разрядная;
- Windows Small Business Server 2003 Standard Service Pack 1 32-разрядная;
- Windows Small Business Server 2003 Premium Service Pack 1 32-разрядная;
- Windows Small Business Server 2008 Standard 64-разрядная;
- Windows Small Business Server 2008 Premium 64-разрядная;
- Microsoft Windows Home Server 2011 64-разрядная;
- Windows MultiPoint Server 2010 Standard 64-разрядная;
- Windows MultiPoint Server 2010 Premium 64-разрядная;
- Microsoft Windows 2000 Server 32-разрядная;

- Windows Server 2003 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Enterprise Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2003 R2 Standard Service Pack 2 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Service Pack 1 Server Core 32-разрядная/64-разрядная;
- Windows Server 2008 Standard Service Pack 1 32-разрядная/64-разрядная;
- Windows Server 2008 Standard 32-разрядная/64-разрядная;
- Windows Server 2008 Enterprise 32-разрядная/64-разрядная;
- Windows Server 2008 Datacenter 32-разрядная/64-разрядная;
- Windows Server 2008 R2 Server Core 64-разрядная;
- Windows Server 2008 R2 Datacenter 64-разрядная;
- Microsoft Windows Server 2008 R2 Enterprise 64-разрядная;
- Windows Server 2008 R2 Foundation 64-разрядная;
- Windows Server 2008 R2 Standard 64-разрядная;
- Windows Server 2016 (вариант установки Nano) (CBB);
- Windows Storage Server 2008 32-разрядная/64-разрядная;
- Windows Storage Server 2008 Service Pack 2 64-разрядная;
- Windows Storage Server 2008 R2 64-разрядная;
- Debian GNU/Linux 7.x (до 7.8) 32-разрядная/64-разрядная;
- Debian GNU/Linux 8.x (Jessie) 32-разрядная/64-разрядная;
- Ubuntu Server 14.04 LTS (Trusty Tahr) 32-разрядная/64-разрядная;
- Ubuntu Server 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная;
- Ubuntu Desktop 14.04 LTS (Trusty Tahr) 32-разрядная/64-разрядная;
- Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-разрядная/64-разрядная;
- CentOS 6.x (до 6.6) 64-разрядная;
- CentOS 8.x 64-разрядная;
- Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная;
- SUSE Linux Enterprise Desktop 12 (все пакеты обновлений) 64-разрядная;
- Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
- Astra Linux Special Edition 4.7 ARM;
- ROSA Enterprise Linux Server 7.3 64-разрядная;
- ROSA Linux Enterprise Desktop 7.3 64-разрядная;

- РОСА "КОБАЛЬТ" Рабочая станция 7.3 64-разрядная;
- РОСА "КОБАЛЬТ" Сервер 7.3 64-разрядная;
- OS X 10.10 (Yosemite);
- OS X 10.11 (El Capitan).

Следующие платформы виртуализации не поддерживаются:

- VMware vSphere 4.1;
- VMware vSphere 5.0;
- VMware vSphere 5.1;
- VMware vSphere 5.5;
- VMware vSphere 7.0;
- VMware vSphere 6.5;
- VMware Workstation 9.x;
- VMware Workstation 10.x;
- VMware Workstation 11.x;
- VMware Workstation 12.x Pro;
- VMware Workstation Pro 14;
- VMware Workstation Pro 15;
- Microsoft Hyper-V Server 2008 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 64-разрядная;
- Microsoft Hyper-V Server 2008 R2 Service Pack 1 64-разрядная;
- Citrix XenServer 6.0;
- Citrix XenServer 6.1;
- Citrix XenServer 6.2;
- Citrix XenServer 6.5;
- Citrix XenServer 7.

## Список поддерживаемых программ "Лаборатории Касперского" и решений

Kaspersky Security Center поддерживает централизованное развертывание и управление всеми поддерживаемыми на данный момент программами и решениями "Лаборатории Касперского". В таблице ниже показано, какие программы и решения "Лаборатории Касперского" поддерживаются Консолью администрирования на основе MMC и Kaspersky Security Center 14.2 Web Console. Подробнее о версиях программ и решений см. на странице "Жизненный цикл программ" https://support.kaspersky.com/corporate/lifecycle.

*Таблица 1. Список программ "Лаборатории Касперского" и решений поддерживаемых программой Kaspersky Security Center*

| Название программы "Лаборатории Касперского" или решения | Поддерживается Консоль администрирования на основе MMC | Поддерживается Kaspersky Security Center 14.2 Web Console |
|---|---|---|
| **Для рабочих станций** | | |
| Kaspersky Endpoint Security для Windows | ✓ | ✓ |
| Kaspersky Endpoint Security для Linux | ✓ | ✓ |
| Kaspersky Endpoint Security для Linux Elbrus Edition | ✓ | ✓ |
| Kaspersky Endpoint Security для Linux ARM Edition | ✓ | ✓ |
| Kaspersky Endpoint Security для Mac | ✓ | ✓ |
| Kaspersky Endpoint Agent | ✓ | ✓ |
| Kaspersky Embedded Systems Security для Windows | ✓ | ✓ |
| **Для промышленных решений** | | |
| Kaspersky Industrial CyberSecurity for Nodes | ✓ | ✓ |
| Kaspersky Industrial CyberSecurity for Linux Nodes | ✓ | ✓ |
| Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается) | ✓ | ✓ |
| **Для мобильных устройств** | | |
| Kaspersky Endpoint Security для Android | ✓ | ✓ |
| Kaspersky Security для iOS | — | ✓ |
| **Для файловых серверов** | | |
| Kaspersky Security для Windows Server | ✓ | ✓ |

| Название программы "Лаборатории Касперского" или решения | Поддерживается Консоль администрирования на основе MMC | Поддерживается Kaspersky Security Center 14.2 Web Console |
|---|---|---|
| Kaspersky Endpoint Security для Windows | ✓ | ✓ |
| Kaspersky Endpoint Security для Linux | ✓ | ✓ |
| **Для виртуальных сред** | | |
| Kaspersky Security для виртуальных сред Легкий агент | ✓ | ✓ |
| Kaspersky Security для виртуальных сред Защита без агента | ✓ | — |
| **Для почтовых систем серверов совместной работы** | | |
| Kaspersky Security для Linux Mail Server | ✓ | — |
| Kaspersky Security для Microsoft Exchange Servers | ✓ | — |
| **Для обнаружения целевых атак** | | |
| Kaspersky Sandbox 2.0 | — | ✓ |
| Kaspersky Endpoint Detection and Response Optimum | — | ✓ |
| Kaspersky Managed Detection and Response | — | ✓ |
| **Для устройств с операционной системой KasperskyOS** | | |
| Kaspersky IoT Secure Gateway | — | ✓ |
| KasperskyOS for Thin Client | — | ✓ |

## См. также:

Основной сценарий установки.....92

kaspersky

# Kaspersky Security Center

В этом руководстве представлена информация о Kaspersky Security Center.

## В этом разделе



# О Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и компонентах программы Kaspersky Security Center, а также способы приобретения Kaspersky Security Center.

kaspersky

Информация в онлайн-справке может отличаться от информации в документах, входящих в состав комплекта документов к программе. В этом случае актуальной считается информация в настоящем руководстве по эксплуатации. Перейти в онлайн-справку можно по ссылкам, встроенным в интерфейс программы, или по ссылке из документации. Онлайн-справка может обновляться без уведомления. При необходимости вы можете переключаться между онлайн-справкой и офлайн-справкой (см. стр. 835).

Программа Kaspersky Security Center является средством антивирусной защиты типа «А» и предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Программа предоставляет администратору доступ к детальной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Программа Kaspersky Security Center адресована администраторам сетей организаций и сотрудникам, отвечающим за защиту устройств в организациях.

В программе Kaspersky Security Center реализованы следующие функции безопасности:

- аудит безопасности программы;
- управление безопасностью;
- сигнализация;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных программ (вирусов) (БД ПКВ);
- централизованная установка компонентов САВЗ.

При помощи Kaspersky Security Center вы можете:

- Формировать иерархию Серверов администрирования для управления сетью собственной организации, а также сетями удаленных офисов или организаций-клиентов.

  Под *организациями-клиентами* здесь подразумеваются организации, антивирусную защиту которых обеспечивает поставщик услуг.
- Формировать иерархию групп администрирования для управления набором клиентских устройств как единым целым.
- Управлять системой антивирусной безопасности, построенной на основе программ "Лаборатории Касперского".
- Централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ "Лаборатории Касперского" и других производителей программного обеспечения.
- Удаленно управлять программами "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах: устанавливать обновления, искать и закрывать уязвимости.
- Централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе программ и устройств.
- Получать уведомления о критических событиях в работе программ "Лаборатории Касперского".
- Управлять мобильными устройствами.

- Управлять шифрованием информации, хранящейся на жестких дисках устройств и съемных дисках, и доступом пользователей к зашифрованным данным.
- Проводить инвентаризацию оборудования, подключенного к сети организации.
- Централизованно работать с файлами, помещенными программами безопасности на карантин или в резервное хранилище, а также с файлами, обработка которых отложена программами безопасности.

Вы можете приобрести Kaspersky Security Center через "Лабораторию Касперского" (например, на сайте https://www.kaspersky.ru) или через компании-партнеров.

Если вы покупаете Kaspersky Security Center через "Лабораторию Касперского", вы можете скачать программу с нашего сайта. Информация, необходимая для активации программы, высылается вам по электронной почте после оплаты.

### В этом разделе



## Лицензии и возможности Kaspersky Security Center

Kaspersky Security Center требует лицензии на некоторые его функции.

В таблице ниже показано, какая лицензия охватывает какие функции Kaspersky Security Center.

*Таблица 2. Лицензии и возможности Kaspersky Security Center*

| Функции Kaspersky Security Center | Системное администрирование | Kaspersky Endpoint Security для бизнеса Расширенный | Kaspersky Endpoint Security для бизнеса | Kaspersky Total Security для бизнеса | Kaspersky Hybrid Cloud Security Standard | Kaspersky Hybrid Cloud Security Enterprise | Kaspersky EDR Optimum |
|---|---|---|---|---|---|---|---|
| Поиск уязвимости (см. стр. 487) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Управление патчами (см. стр. 477) | ✓ | — | ✓ | ✓ | — | ✓ | ✓ |

| Функции Kaspersky Security Center | Системное администрирование | Kaspersky Endpoint Security для бизнеса | Kaspersky Endpoint Security для бизнеса Расширенный | Kaspersky Total Security для бизнеса | Kaspersky Hybrid Cloud Security Standard | Kaspersky Hybrid Cloud Security Enterprise | Kaspersky EDR Optimum |
|---|---|---|---|---|---|---|---|
| Управление доступом на основе ролей (см. стр. 771) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Установка операционных систем и программ (см.стр. 803) | ✓ | — | ✓ | ✓ | — | ✓ | ✓ |
| Управление мобильными устройствами (то есть управление iOS- и Android-устройствами пользователей) | ✓ | ✓ | ✓ | ✓ | — | — | ✓ |
| Настройка облачного окружения для работы в облачных окружениях, таких как AWS, Microsoft Azure или Google Cloud | — | — | — | — | ✓ | ✓ | — |

| Функции Kaspersky Security Center | Системное администрирование | Kaspersky Endpoint Security для бизнеса Расширенный | Kaspersky Endpoint Security для бизнеса Расширенный | Kaspersky Total Security для бизнеса | Kaspersky Hybrid Cloud Security Standard | Kaspersky Hybrid Cloud Security Enterprise | Kaspersky EDR Optimum |
|---|---|---|---|---|---|---|---|
| Экспорт событий в SIEM-системы: Syslog (см.стр. 846) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Экспорт событий в SIEM-системы: QRadar от IBM и Micro Focus от Micro Focus(см.стр. 846) | ✓ | — | ✓ | ✓ | — | ✓ | ✓ |

См. также:



# О совместимости Сервера администрирования и Kaspersky Security Center 14.2 Web Console

Рекомендуется использовать последние версии Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console; в противном случае функциональность Kaspersky Security Center может быть ограничена.

Вы можете установить и обновить Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console независимо друг от друга. В этом случае убедитесь, что версия установленной программы Kaspersky Security Center Web Console совместима с версией Сервера администрирования, к которому вы подключаетесь:

- Kaspersky Security Center 14.2 Web Console поддерживает Сервер администрирования Kaspersky Security Center следующих версий: 14.2, 14 и 13.2.
- Сервер администрирования Kaspersky Security Center 14.2 поддерживает Kaspersky Security Center Web Console следующих версий: 14.2, 14 и 13.2.

# Сравнение версий Kaspersky Security Center: на базе Windows и на базе Linux

"Лаборатории Касперского" предлагает программу Kaspersky Security Center в качестве локального решения для двух платформ – Windows и Linux. В решении для Windows вы устанавливаете Сервер администрирования на устройство с операционной системой Windows. Решение на базе Linux имеет версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Эта онлайн-справка содержит информацию о Kaspersky Security Center Windows. Для получения подробной информации о решении на базе Linux см. онлайн-справку Kaspersky Security Center Linux https://support.kaspersky.com/KSCLinux/14/ru-RU/5022.htm.

Таблица ниже позволяет сравнить основные возможности Kaspersky Security Center как решения на базе Windows и как решения на базе Linux.

*Таблица 3. Сравнение возможностей программы Kaspersky Security Center на базе Windows и на базе Linux*

| Функция или свойство | Kaspersky Security Center 14.2 | |
|---|---|---|
| | Решение на базе Windows | Решение на базе Linux |
| Расположение Сервера администрирования | Локально | Локально |
| Расположение системы управления базами данных (СУБД) | Локально | Локально |
| Операционная система для установки Сервера администрирования | Windows | Linux |
| Тип Консоли администрирования | Локальная и веб-интерфейс | Веб-интерфейс |
| Операционная система для установки Консоли администрирования с веб-интерфейсом | Windows или Linux | Windows или Linux |
| Иерархия Серверов администрирования | ✓ | ✓ |
| Иерархия групп администрирования | ✓ | ✓ |
| Опрос сети | ✓ | ✓ (только по IP-диапазонам) |
| Максимальное количество управляемых устройств | 100 000 | 20 000 |

| Функция или свойство | Kaspersky Security Center 14.2 | |
|---|---|---|
| | Решение на базе Windows | Решение на базе Linux |
| Защита устройств под управлением Windows, macOS и Linux | ✓ | ✓ (защита устройств только с операционными системами Linux и Windows) |
| Защита мобильных устройств | ✓ | — |
| Защита виртуальных машин | ✓ | — |
| Защита публичной облачной инфраструктуры | ✓ | — |
| Управление безопасностью, ориентированное на устройства (см. стр. 1078) | ✓ | ✓ |
| Управление безопасностью, ориентированное на пользователя (см. стр. 1078) | ✓ | ✓ |
| Политики программ | ✓ | ✓ |
| Задачи для программ "Лаборатории Касперского" | ✓ | ✓ |
| Kaspersky Security Network | ✓ | ✓ |
| Прокси-сервер KSN | ✓ | ✓ |
| Kaspersky Private Security Network | ✓ | ✓ |
| Централизованное распространение лицензионных ключей программ "Лаборатории Касперского" | ✓ | ✓ |
| Автоматическое обновление антивирусных баз | ✓ | ✓ |
| Поддержка виртуальных Серверов администрирования | ✓ | ✓ |
| Установка обновлений программ сторонних производителей и поиск уязвимостей в программах сторонних производителей | ✓ | — (только с помощью задачи удаленной установки) |

| Функция или свойство | Kaspersky Security Center 14.2 | |
|---|---|---|
| | Решение на базе Windows | Решение на базе Linux |
| Уведомления о событиях, произошедших на управляемых устройствах | ✓ | ✓ |
| Создание учетных записей пользователей, контроль учетных записей | ✓ | ✓ |
| Вход в консоль с использованием доменной аутентификации | ✓ | — |
| Интеграция с SIEM-системами | ✓ | ✓ (только с использованием Syslog) |
| Мониторинг состояния политик и задач | ✓ | ✓ |
| Развертывание отказоустойчивого кластера "Лаборатории Касперского" | ✓ | ✓ |
| Установка Сервера администрирования на отказоустойчивом кластере Microsoft | ✓ | — |
| Использование SNMP для отправки статистики Сервера администрирования программам сторонних производителей | ✓ | — |
| Удаленная диагностика клиентских устройств | ✓ | — |
| Удаленное подключение к рабочему столу клиентского устройства | ✓ | — |
| Работа с ревизиями объектов | ✓ | — |
| Автоматическое обновление программ "Лаборатории Касперского" | ✓ | — |
| Развертывание операционных систем на клиентских устройствах | ✓ | — |

| Функция или свойство | Kaspersky Security Center 14.2 | |
|---|---|---|
| | Решение на базе Windows | Решение на базе Linux |
| Веб-сервер для публикации инсталляционных пакетов и других файлов | ✓ | — |
| Просмотр и работа с обнаружениями, зарегистрированными Kaspersky Endpoint Detection and Response Optimum | ✓ | — |
| Использовать Сервер администрирования в роли WSUS-сервера | ✓ | — |
| Интеграция с Kaspersky Managed Detection and Response | ✓ | — |
| Поддержка Адаптивного контроля аномалий | ✓ | — |
| Поддержка кластеров и массивов серверов в группах администрирования | ✓ (только в Консоли администрирования на основе MMC) | — |
| Управление сторонними лицензиями | ✓ | — |

kaspersky

# Основные понятия

Этот раздел содержит развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

## В этом разделе



## Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

Устройства, на которых установлен компонент Сервер администрирования, называются *Серверами администрирования* (далее также *Серверами*). Серверы администрирования должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

Сервер администрирования устанавливается на устройство в качестве службы со следующим набором атрибутов:

- под именем "Сервер администрирования Kaspersky Security Center";
- с автоматическим типом запуска при старте операционной системы;

- с учетной записью **LocalSystem** либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;
- обновление баз и модулей программ "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе программ "Лаборатории Касперского";
- распространение лицензионных ключей на клиентские устройства, хранение информации о ключах;
- отправка уведомлений о ходе выполнения задач (например, об обнаружении вирусов на клиентском устройстве).

**Правило именования Серверов администрирования в интерфейсе программы**

В интерфейсе Консоли администрирования и Kaspersky Security Center 14.2 Web Console Серверы администрирования могут иметь следующие имена:

- Имя устройства Сервера администрирования, например: "*имя_устройства*" или "Сервер администрирования: *имя_устройства*".
- IP-адрес устройства Сервера администрирования, например: "*IP_адрес*" или "Сервер администрирования: *IP_адрес* ".
- Подчиненные Серверы администрирования и виртуальные Серверы администрирования имеют собственные имена, которые вы указываете при подключении виртуального или подчиненного Сервера администрирования к главному Серверу администрирования.
- Если вы используете программу Kaspersky Security Center 14.2 Web Console, установленную на устройство под управлением Linux, то программа отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов (см. стр. 955).

Вы можете подключиться к Серверу администрирования с помощью Консоли администрирования (см. стр. 138) или с помощью Kaspersky Security Center 14.2 Web Console.

## См. также:

Основной сценарий установки.....92

Установка Kaspersky Security Center.....217

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения.....136

kaspersky

## Иерархия Серверов администрирования

Вы можете объединять Серверы администрирования в иерархию. Каждый Сервер администрирования может иметь несколько подчиненных Серверов администрирования (далее также *подчиненных Серверов*) на разных уровнях иерархии. Уровень вложенности подчиненных Серверов не ограничен. При этом в состав групп администрирования главного Сервера будут входить клиентские устройства всех подчиненных Серверов. Таким образом, независимые участки компьютерной сети могут управляться различными Серверами администрирования, которые, в свою очередь, управляются главным Сервером.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. стр. 78).

Иерархию Серверов администрирования можно использовать для следующих целей:

- Ограничение нагрузки на Сервер администрирования (по сравнению с одним установленным в сети Сервером).
- Сокращение трафика внутри сети и упрощение работы с удаленными офисами. Нет необходимости устанавливать соединение между главным Сервером и всеми устройствами сети, которые могут находиться, например, в других регионах. Достаточно установить на каждом участке сети подчиненный Сервер администрирования, распределить устройства в группах администрирования подчиненных Серверов и обеспечить подчиненным Серверам соединение с главным Сервером по быстрым каналам связи.
- Разделение ответственности между администраторами антивирусной безопасности. При этом сохраняются все возможности централизованного управления и мониторинга состояния антивирусной безопасности сети организации.

Каждое устройство, включенное в иерархию групп администрирования, может быть подключено только к одному Серверу администрирования. Вам нужно самостоятельно проверять подключение устройств к Серверам администрирования. Для этого можно использовать функцию поиска устройств по сетевым атрибутам в группах администрирования различных Серверов.

### См. также:

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования ..... 141

## Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент программы Kaspersky Security Center, предназначенный для управления сетью организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также

задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.

- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки программ "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.
- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center перезапускает главный Сервер администрирования и все виртуальные Серверы.

Администратор виртуального Сервера обладает всеми правами в рамках этого виртуального Сервера.

## Сервер мобильных устройств

*Сервер мобильных устройств* – это компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

Существуют два вида Серверов мобильных устройств:

- Сервер мобильных устройств Exchange ActiveSync. Устанавливается на устройство, на котором установлен сервер Microsoft Exchange, и позволяет получать данные с сервера Microsoft Exchange и передавать их на Сервер администрирования. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими протокол Exchange ActiveSync.
- Сервер iOS MDM. Этот Сервер мобильных устройств используется для управления мобильными устройствами, поддерживающими Apple® Push Notifications (APNs).

Серверы мобильных устройств Kaspersky Security Center позволяют управлять следующими объектами:

- Отдельным мобильным устройством.
- Несколькими мобильными устройствами.
- Несколькими мобильными устройствами, подключенными к кластеру серверов, одновременно. При подключении к кластеру серверов Сервер мобильных устройств, установленный на этом кластере, отображается в Консоли администрирования как один сервер.

## Веб-сервер

*Веб-сервер* Kaspersky Security Center (далее также *Веб-сервер*) – это компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи

по сети автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию автономного пакета или повторно опубликовать его на Веб-сервере.

При создании iOS MDM-профиль для мобильного устройства пользователя также автоматически публикуется на Веб-сервере. Опубликованный профиль автоматически удаляется с Веб-сервера после успешной установки на мобильное устройство пользователя.

Папка общего доступа используется для размещения информации, доступной всем пользователям, устройства которых находятся под управлением Сервера администрирования. Если у пользователя нет прямого доступа к папке общего доступа, ему можно передать информацию из этой папки с помощью Веб-сервера.

Для передачи пользователям информации из папки общего доступа с помощью Веб-сервера администратору требуется создать в папке общего доступа вложенную папку public и поместить в нее информацию.

Синтаксис ссылки для передачи информации пользователю выглядит следующим образом:

```
https://<имя Веб-сервера>:<порт HTTPS>/public/<объект>
```

где

- `<имя Веб-сервера>` – имя Веб-сервера Kaspersky Security Center.
- `<порт HTTPS>` – HTTPS-порт Веб-сервера, заданный администратором. HTTPS-порт можно задать в разделе **Веб-сервер** окна свойств Сервера администрирования. По умолчанию установлен порт 8061.
- `<объект>` – вложенная папка или файл, доступ к которым требуется открыть для пользователя.

Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

По полученной ссылке пользователь может загрузить на локальное устройство предназначенную для него информацию.

## Агент администрирования

Взаимодействие между Сервером администрирования и устройствами обеспечивается *Агентом администрирования* – компонентом Kaspersky Security Center. Агент администрирования требуется установить на все устройства, на которых управление работой программ "Лаборатории Касперского" выполняется с помощью Kaspersky Security Center.

Агент администрирования устанавливается на устройстве в качестве службы со следующим набором атрибутов:

- под именем "Агент администрирования Kaspersky Security Center";
- с автоматическим типом запуска при старте операционной системы;
- с помощью учетной записи LocalSystem.

Устройство, на которое установлен Агент администрирования, называется *управляемым устройством* или *устройством*.

Агент администрирования можно установить на устройство под управлением операционной системы Windows, Linux или Mac. Вы можете активировать компонент следующими способами:

- Инсталляционный пакет в хранилище Сервера администрирования (необходимо, чтобы был установлен Сервер администрирования).
- Инсталляционный пакет находится на веб-серверах "Лаборатории Касперского" (см. стр. 381).

Нет необходимости устанавливать Агент администрирования на устройства, на которых установлен Сервер администрирования, поскольку серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования.

Название процесса, который запускает Агент администрирования, – *klnagent.exe*.

Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (*периодический сигнал*) равным 15 минут на 10 000 управляемых устройств.

### См. также:

Параметры политики Агента администрирования ..... 750

Развертывание Агента администрирования и программы безопасности ..... 178

## Группы администрирования

*Группа администрирования* (далее также *группа*) – это набор клиентских устройств, объединенных по какому-либо признаку с целью управления устройствами группы как единым целым в Kaspersky Security Center

Для всех клиентских устройств в группе устанавливаются:

- Единые параметры работы программ – с помощью групповых политик.
- Единый режим работы всех программ – с помощью создания групповых задач с определенным набором параметров. Примеры групповых задач включают создание и установку общего инсталляционного пакета, обновление баз и модулей программы, проверку устройства по требованию и включение постоянной защиты.

Клиентское устройство может входить в состав только одной группы администрирования.

Для Серверов администрирования и групп администрирования можно создавать иерархии с любым уровнем вложенности. На одном уровне иерархии могут располагаться подчиненные и виртуальные Серверы администрирования, группы и клиентские устройства. Можно переводить устройства из одной группы в другую, не перемещая их физически. Например, если сотрудник предприятия перешел с позиции бухгалтера на позицию разработчика, вы можете перевести компьютер этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, на компьютер будут автоматически переданы настойки программ, необходимые для позиции разработчика.

### См. также:

Управление группами администрирования ..... 708

## Управляемое устройство

*Управляемое устройство* – это компьютер под управлением Windows, Linux или macOS, на котором установлен Агент администрирования, или мобильное устройство, на котором установлено приложение безопасности "Лаборатории Касперского". Вы можете управлять такими устройствами с помощью задач и политик для программ, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

Вы можете настроить управляемое немобильное устройство, чтобы оно выполняло функции точки распространения и шлюза соединений.

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 100 000 устройств, включая мобильные устройства.

## Нераспределенное устройство

*Нераспределенное устройство* – это устройство в сети, которое не включено ни в одну из групп администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них программы.

Когда в сети обнаруживается новое устройство, оно помещается в группу администрирования Нераспределенные устройства. Можно настроить правила автоматического распределения устройств по группам администрирования в момент обнаружения.

## Рабочее место администратора

*Рабочее место администратора* — устройство, на котором установлена Консоль администрирования или которое вы используете для работы с Kaspersky Security Center 14.2 Web Console. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Найдите его в меню **Пуск → Программы → Kaspersky Security Center**.

Количество рабочих мест администратора не ограничивается. С каждого рабочего места администратора можно управлять группами администрирования сразу нескольких Серверов администрирования в сети. Рабочее место администратора можно подключить к Серверу администрирования (как к физическому, так и к виртуальному) любого уровня иерархии.

Рабочее место администратора можно включить в состав группы администрирования в качестве клиентского устройства.

В пределах групп администрирования любого Сервера одно и то же устройство может быть одновременно и клиентом Сервера администрирования, и Сервером администрирования, и рабочим местом администратора.

## Плагин управления

Управление программами "Лаборатории Касперского" через Консоль администрирования выполняется при помощи специального компонента – *плагина управления*. В состав каждой программы "Лаборатории Касперского", которой можно управлять при помощи Kaspersky Security Center, входит плагин управления.

С помощью плагина управления программой в Консоли администрирования можно выполнять следующие

действия:

- создавать и редактировать политики и параметры программы, а также параметры задач этой программы;
- получать информацию о задачах программы, событиях в ее работе, а также о статистике работы программы, получаемой с клиентских устройств.

Плагины управления сертифицируемых программ «Лаборатории Касперского» распространяются в составе соответствующих дистрибутивов программ, для управления которыми они предназначены.

## Веб-плагин управления

*Веб-плагин управления* – это специальный компонент, используемый для удаленного управления программами "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console. Веб-плагин управления также называется *плагином управления*. Плагин управления представляет собой интерфейс между Kaspersky Security Center 14.2 Web Console и определенной программой "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для программы.

Вы можете загрузить веб-плагины управления с веб-сайта Службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/9333.

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач (на стр. 1108) и параметров программы.
- Интерфейс для создания и изменения политик и профилей политик (см. стр. 426) для удаленной централизованной настройки программ "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных программами.
- Функции Kaspersky Security Center 14.2 Web Console для отображения оперативных данных и событий программы, а также статистики, полученной от клиентских устройств.

### См. также:

Плагин управления ..... 82

О Kaspersky Security Center 14.2 Web Console ..... 942

Развертывание программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console ..... 1035

## Политики

*Политика* – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 81) и ее подгруппам. Вы можете установить несколько программ "Лаборатории Касперского" (см. стр. 69) на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждой программы "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

*Таблица 4. Статус политики*

| Состояние | Описание |
|---|---|
| Активная | Это текущая политика, которая применяется к устройству. Для программы "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики программы "Лаборатории Касперского" применяются к устройству. |
| Неактивная | Политика, которая в настоящее время не применяется к устройству. |
| Для автономных пользователей | Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. |

Политики действуют по следующим правилам:

- Для одной программы можно настроить несколько политик с различными значениями.
- Для одной программы может быть активна только одна политика.
- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

*Профиль политики* – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локальной программы, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

## См. также:

Основной сценарий установки.....92

Политики и профили политик .....426

Создание политики .....1174

kaspersky

## Профили политик

Может возникнуть необходимость создать несколько копий одной политики для разных групп администрирования; может также возникнуть необходимость централизованно изменить параметры этих политик. Эти копии могут различаться одним или двумя параметрами. Например, все бухгалтеры в организации работают под управлением одной и той же политики, но старшим бухгалтерам разрешено использовать флеш-накопители USB, а младшим бухгалтерам не разрешено. В этом случае применение политик к устройствам только через иерархию групп администрирования может оказаться неудобным.

Чтобы избежать создания нескольких копий одной политики, Kaspersky Security Center позволяет создавать *профили политик*. Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики.

Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве. При активации профиля изменяются параметры "базовой" политики, которые исходно действовали на устройстве. Эти параметры принимают значения, указанные в профиле.

### См. также:


Политики и профили политик ..... 426

Создание профиля политики ..... 1184


## Задачи

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Вы можете создать задачу для программы, только если для этой программы установлен плагин управления.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждой программы вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и Kaspersky Security Center (см. стр. 1376) как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

### См. также:



## Область действия задачи

*Область задачи* (см. стр. 1109) – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

  Задачи будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

## Взаимосвязь политики и локальных параметров программы

Вы можете при помощи политик устанавливать одинаковые значения параметров работы программы для всех устройств, входящих в состав группы.

Переопределить значения параметров, заданные политикой, для отдельных устройств в группе можно при помощи локальных параметров программы. При этом можно установить значения только тех параметров, изменение которых не запрещено политикой (параметр не закрыт замком).

Значение параметра, которое использует программа на клиентском устройстве, определяется наличием замка (  ) у параметра в политике:

- Если на изменение параметра наложен запрет, на всех клиентских устройствах используется одно и то же заданное политикой значение.
- Если запрет не наложен, то на каждом клиентском устройстве программа использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры программы.

Таким образом, при выполнении задачи на клиентском устройстве программа использует параметры, заданные двумя разными способами:

- параметрами задачи и локальными параметрами программы, если в политике не был установлен запрет на изменение параметра;
- политикой группы, если в политике был установлен запрет на изменение параметра.

Локальные параметры программы изменяются после первого применения политики в соответствии с параметрами политики.

См. также:

Политики и профили политик .....426

## Точка распространения

*Точка распространения* (ранее называлась "агент обновлений") – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в сети. Точка распространения может выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства группы (в том числе и с помощью широковещательной рассылки по протоколу UDP). Обновления могут быть получены как с Сервера администрирования, так и с серверов обновлений "Лаборатории Касперского". В последнем случае для точки распространения должна быть создана задача обновления (см. стр. 473).

  Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

  > Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

  Точки распространения ускоряют распространение обновлений и позволяют высвободить ресурсы Сервера администрирования.

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.

- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования (см. стр. 667).

  Если нет возможности создать прямое соединение между управляемыми устройствами группы и Сервером администрирования, точку распространения можно назначить шлюзом соединений этой группы с Сервером администрирования. В этом случае управляемые устройства подключаются к шлюзу соединений, который, в свою очередь, подключается к Серверу администрирования.

  Наличие точки распространения, работающей в режиме шлюза соединений не исключает прямого соединения управляемых устройств с Сервером администрирования. Если шлюз соединений недоступен, а прямое соединение с Сервером администрирования технически возможно, управляемые устройства напрямую подключаются к Серверу.

- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

- Выполнять удаленную установку программ сторонних производителей и программ "Лаборатории Касперского" средствами операционной системы точки распространения. Обратите внимание, что точка распространения может выполнять установку на клиентские устройства без Агента администрирования.

Эта функция позволяет удаленно передавать инсталляционные пакеты Агента администрирования на клиентские устройства, расположенные в сетях, к которым у Сервера администрирования нет прямого доступа.

- Выступать в роли прокси-сервера, участвующего в Kaspersky Security Network (KSN).

  Можно включить прокси-сервер KSN на стороне точки распространения (см. стр. 481), чтобы устройство исполняло роль прокси-сервера KSN. В этом случае на устройстве запустится служба прокси-сервера KSN (ksnproxy) (см. стр. 277).

Передача файлов от Сервера администрирования точке распространения осуществляется по протоколу HTTP или, если настроено использование SSL-соединения, по протоколу HTTPS. Использование протокола HTTP или HTTPS обеспечивает более высокую производительность по сравнению с использованием протокола SOAP за счет сокращения трафика.

Устройства с установленным Агентом администрирования могут быть назначены точками распространения вручную администратором (см. стр. 481) или автоматически Сервером администрирования. Полный список точек распространения для указанных групп администрирования отображается в отчете со списком точек распространения.

Областью действия точки распространения является группа администрирования, для которой она назначена администратором, а также ее подгруппы всех уровней вложенности. Если в иерархии групп администрирования назначено несколько точек распространения, Агент администрирования управляемого устройства подключается к наиболее близкой по иерархии точке распространения.

Областью действия точек распространения также может являться сетевое местоположение. Сетевое местоположение используется для формирования вручную набора устройств, на которые точка распространения будет распространять обновления. Определение сетевого местоположения доступно только для устройств под управлением операционной системы Windows.

Если точки распространения назначаются автоматически Сервером администрирования, то Сервер назначает точки распространения по широковещательным доменам, а не по группам администрирования. Это происходит после того, как становятся известны широковещательные домены. Агент администрирования обменивается с другими Агентами администрирования своей подсети сообщениями и отправляет Серверу администрирования информацию о себе и краткую информацию о других Агентах администрирования. На основании этой информации Сервер администрирования может сгруппировать Агенты администрирования по широковещательным доменам. Широковещательные домены становятся известны Серверу администрирования после того, как опрошено более 70% Агентов администрирования в группах администрирования. Сервер администрирования опрашивает широковещательные домены каждые два часа. После того как точки распространения назначены по широковещательным доменам, их нельзя назначить снова по группам администрирования.

Если администратор вручную назначает точки распространения, их можно назначать группам администрирования или сетевым местоположениям.

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.
Kaspersky Security Center присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с

Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

Статус точки распространения (*Активный* / *Резервный*) отображается флажком в отчете утилиты klnagchk (см. стр. 722).

Для работы точки распространения требуется не менее 4 ГБ свободного места на диске. Если объем свободного места на диске точки распространения меньше 2 ГБ, Kaspersky Security Center создает инцидент с уровнем важности *Предупреждение*. Инцидент будет опубликован в свойствах устройства в разделе **Инциденты**.

При работе задач удаленной установки на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть больше размера всех устанавливаемых инсталляционных пакетов.

При работе задачи установки обновлений (патчей) и закрытия уязвимостей на устройстве с точкой распространения потребуется дополнительное свободное дисковое пространство. Свободное дисковое пространство должно быть как минимум в два раза больше размера всех устанавливаемых патчей.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

### См. также:


Настройка точек распространения и шлюзов соединений ..... 658

О точках распространения ..... 167

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449


## Шлюз соединения

*Шлюз соединения* – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

Шлюз соединения может принимать соединения от 10 000 устройств.

Существует два варианта использования шлюзов соединения:

- Рекомендуется установить шлюз соединения в демилитаризованной зоне (DMZ). Для других Агентов администрирования, установленных на автономных устройствах (см. стр. 304), необходимо специально настроить подключение к Серверу администрирования через шлюз соединения.

  Шлюз соединения не изменяет и не обрабатывает данные, передаваемые от Агентов администрирования на Сервер администрирования. Шлюз соединения не записывает эти данные в буфер и, следовательно, не может принимать данные от Агента администрирования и затем

передавать их на Сервер администрирования. Если Агент администрирования пытается подключиться к Серверу администрирования через шлюз соединения, но шлюз соединения не может подключиться к Серверу администрирования, Агент администрирования воспринимает это как недоступный Сервер администрирования. Все данные остаются на Агенте администрирования (не на шлюзе соединения).

Шлюз соединения не может подключиться к Серверу администрирования через другой шлюз соединения. Это означает, что Агент администрирования не может одновременно быть шлюзом соединения и использовать шлюз соединения для подключения к Серверу администрирования.

Все шлюзы соединения включены в список точек распространения в свойствах Сервера администрирования.

- Вы также можете использовать шлюзы соединения в сети. Например, автоматически назначаемые точки распространения также становятся шлюзами соединений в своей области действия. Однако во внутренней сети шлюзы соединения не дают значительных преимуществ. Они уменьшают количество сетевых подключений, принимаемых Сервером администрирования, но не уменьшают объем входящих данных. Даже без шлюзов соединения все устройства могли подключаться к Серверу администрирования.

### См. также:

Настройка точек распространения и шлюзов соединений .....658

Об использовании точки распространения в качестве шлюза соединений.....667

# Архитектура программы

Этот раздел описывает архитектуру и основные понятия Kaspersky Security Center.

Программа Kaspersky Security Center включает в себя следующие основные компоненты:

- **Сервер администрирования** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.
- **Агент администрирования** (далее также *Агент*). Осуществляет взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft® Windows®. Для программ "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.
- **Консоль администрирования** (далее также *Консоль*). Предоставляет пользовательский интерфейс к административным службам Сервера и Агента. Консоль администрирования выполнена в виде компонента расширения к Microsoft Management Console (MMC). Консоль администрирования позволяет подключаться к удаленному Серверу администрирования через интернет.
- **Сервер мобильных устройств**. Предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования. Сервер мобильных устройств получает информацию о мобильных устройствах и хранит их профили.

kaspersky

См. также:

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения .....136

# Основной сценарий установки

Следуя основному сценарию, вы можете развернуть Сервер администрирования, а также установить на устройства сети Агент администрирования и программы безопасности. Вы можете использовать этот сценарий и для ознакомления с программой, и для установки программы с целью дальнейшей работы.

Информацию о развертывании Kaspersky Security Center Cloud Console см. в документации Kaspersky Security Center Cloud Console https://help.kaspersky.com/KSC/CloudConsole/ru-RU/153504.htm.

Установка Kaspersky Security Center включает следующие шаги:

1. Подготовка.
2. Установка Kaspersky Security Center и программ безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования
3. Удаленное развертывание программ безопасности "Лаборатории Каперского" на клиентских устройствах

Развертывание Kaspersky Security Center в облачном окружении и развертывание Kaspersky Security Center для поставщиков услуг описаны в соответствующих разделах справки.

Рекомендуется отвести на установку Сервера администрирования не менее часа, а на выполнение сценария целиком – не менее одного рабочего дня. На компьютер, который будет выполнять роль Сервера администрирования Kaspersky Security Center, также рекомендуется установить программу безопасности, например, Kaspersky Security для Windows Server или Kaspersky Endpoint Security.

После завершения сценария в сети организации будет развернута защита из следующим способом:

- Для Сервера администрирования будет установлена СУБД.
- Сервер администрирования Kaspersky Security Center будет установлен.
- Все необходимые политики и задачи будут созданы, а также будут настроены заданные по умолчанию параметры политик и задач.
- На управляемые устройства будут установлены программы безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования.
- Группы администрирования будут созданы (возможно, объединенные в иерархию).
- При необходимости будет развернута защита мобильных устройств.
- При необходимости будут назначены точки распространения.

Установка Kaspersky Security Center происходит поэтапно:

**Подготовка.**

a. **Получение необходимых файлов**

   Убедитесь, что у вас есть лицензионный ключ (код активации) для Kaspersky Security Center или лицензионные ключи (коды активации) для программ безопасности "Лаборатории Касперского".

Распакуйте архив, полученный от вашего поставщика. Этот архив содержит лицензионные ключи (файлы формата KEY), коды активации (см. стр. 345) и список программ "Лаборатории Касперского", которые могут быть активированы каждым из этих лицензионных ключей.

Если вы хотите попробовать Kaspersky Security Center, вы можете получить пробную тридцатидневную версию на веб-сайте "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security.

Подробную информацию о лицензировании программ безопасности "Лаборатории Касперского", которые не входят в состав Kaspersky Security Center, вы можете найти в документации к этим программам.

**b. Выбор структуры защиты организации**

Ознакомьтесь с компонентами Kaspersky Security Center (см. стр. 91). Выберите структуру защиты и конфигурацию сети (см. стр. 162), наиболее подходящие для вашей организации. Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам (см. стр. 159), если вы работаете с распределенной сетью.

Для достижения и сохранения оптимальной производительности при различных условиях работы, пожалуйста, учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center (подробнее см. в Руководстве по масштабированию Kaspersky Security Center (см. стр. 1488)).

Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования (см. стр. 78). Для этого нужно понять, возможно и целесообразно ли обслуживание всех клиентских устройств одним Сервером администрирования или требуется выстроить иерархию Серверов администрирования. Вам также может потребоваться выстроить иерархию Серверов администрирования, совпадающую с организационной структурой предприятия, сеть которого вы хотите защитить.

Если вам требуется обеспечить защиту мобильных устройств, выполните подготовительные действия по настройке Сервера мобильных устройств Exchange ActiveSync и Сервера iOS MDM.

Убедитесь, что устройства, выбранные вами для использования в качестве Серверов администрирования, а также для установки Консоли администрирования, соответствуют аппаратным и программным требованиям (на стр. 69).

**c. Подготовка к использованию пользовательских сертификатов**

Если инфраструктура открытых ключей (PKI) вашей организации требует, чтобы вы использовали пользовательские сертификаты, выпущенные определенным аккредитованным центром сертификации (CA), подготовьте эти сертификаты (см. стр. 108) и убедитесь, что они соответствуют всем требованиям (см. стр. 112).

**d. Подготовка к лицензированию Kaspersky Security Center**

Если вы планируете использовать версию Kaspersky Security Center с поддержкой Управления мобильными устройствами, Интеграцией с SIEM-системами и/или с поддержкой Системного администрирования, убедитесь, что у вас имеется файл ключа либо код активации для лицензирования программы (см. стр. 341).

**e. Подготовка к лицензированию управляемых программ безопасности**

Во время развертывания защиты вам потребуется предоставить "Лаборатории Касперского" активные лицензионные ключи на те программы, которыми вы планируете управлять с помощью Kaspersky Security Center (см. список доступных для управления программ безопасности (см. стр. 69)). Подробнее о лицензировании каждой из программ безопасности вы можете прочитать в документации к этим программам.

**f. Выбор аппаратной конфигурации Сервера администрирования и СУБД**

Спланируйте аппаратную конфигурацию для СУБД и Сервера администрирования с учетом количества устройств в вашей сети.

**g. Выбор СУБД**

При выборе СУБД (на стр. 164) учитывайте количество управляемых устройств, которые будет обслуживать Сервер администрирования. Если в вашей сети менее 10 000 устройств и вы не планируете увеличивать их количество, вы можете выбрать бесплатную СУБД SQL Express или MySQL и установить ее на одном устройстве с Сервером администрирования. Вы можете выбрать СУБД MariaDB, которая позволяет управлять устройствами в количестве до 20 000. Если в вашей сети более 10 000 устройств (или вы планируете расширение сети до такого количества устройств), рекомендуется выбирать платную СУБД SQL и размещать ее на отдельном устройстве. Платная СУБД может работать с несколькими Серверами администрирования, а бесплатная СУБД – только с одним.

Если вы выберете SQL Server, тогда можно перенести данные, хранящиеся в базе данных, в MySQL, в MariaDB или в Azure SQL СУБД. Чтобы выполнить перенос данных, выполните резервное копирование данных и восстановите их в новой СУБД (см. стр. 693).

**h. Установка СУБД и создание базы данных**

Узнайте больше об учетных записях для работы с СУБД (на стр. 218) и установите СУБД. Запишите и сохраните параметры СУБД, поскольку они потребуются вам при установке Сервера администрирования. Эти параметры включают имя SQL-сервера, номер порта для подключения к SQL-серверу, имя учетной записи и пароль для доступа к SQL-серверу.

> Если вы решили установить СУБД PostgreSQL или Postgres Pro, убедитесь, что вы указали пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

По умолчанию инсталлятор Kaspersky Security Center создает базу данных для размещения информации Сервера администрирования (см. стр. 247), однако вы можете отказаться от ее создания и использовать другую базу данных. В этом случае убедитесь, что база данных создана, вы знаете ее имя, а учетная запись, под которой Сервер администрирования получит доступ к этой базе данных, будет иметь для нее роль db_owner.

При необходимости обратитесь за информацией к администратору СУБД.

**i. Настройка портов**

Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты (см. стр. 136) открыты необходимые порты (см. стр. 98).

Если требуется предоставить доступ к Серверу администрирования из интернета, настройте порты и параметры подключения в зависимости от конфигурации сети.

**j. Проверка учетных записей**

Проверьте наличие у вас прав локального администратора для успешной установки Сервера администрирования Kaspersky Security Center и развертывания защиты на устройствах. Права локального администратора на клиентских устройствах нужны для установки на эти устройства Агента администрирования. После установки Агента администрирования вы сможете с его помощью удаленно устанавливать программы на устройства, не пользуясь учетной записью с правами администратора устройства.

По умолчанию инсталлятор Kaspersky Security Center создает на устройстве, выбранном для установки Сервера администрирования, три локальные учетные записи, от имени которых будет

запускаться Сервер администрирования (см. стр. 249) и службы Kaspersky Security Center (см. стр. 250):

- KL-AK-*: учетная запись службы Сервера администрирования;

NT Service/KSC*: KlScSvc: учетная запись для прочих служб из состава Сервера администрирования

- KlPxeUser: учетная запись для развертывания операционных систем.

Вы можете отказаться от создания учетных записей для служб Сервера администрирования и других служб. Вместо этого вы можете использовать существующие учетные записи, например учетные записи домена, если планируете установить Сервер администрирования на отказоустойчивом кластере (см. стр. 236) или планируете использовать учетные записи домена вместо локальных учетных записей по другой причине. В этом случае убедитесь, что учетные записи для запуска Сервера администрирования и служб Kaspersky Security Center созданы, являются непривилегированными и обладают необходимыми правами для доступа к СУБД (см. стр. 218). (Если вы планируете в дальнейшем разворачивать операционные системы (см. стр. 808) на устройствах средствами Kaspersky Security Center, не отказывайтесь от создания учетных записей.)

**Установка Kaspersky Security Center и программ безопасности "Лаборатории Касперского" на устройстве с Сервером администрирования**

**a. Установка Сервера администрирования, Консоли администрирования, Kaspersky Security Center 14.2 Web Console и плагинов управления для программ безопасности**

Загрузите Kaspersky Security Center с сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/security-center. Можно загрузить полный пакет, только Kaspersky Security Center Web Console или только Консоль администрирования.

Установите Сервер администрирования (см. стр. 217) на устройство, которое вы выбрали (либо устройства, если вы планируете (см. стр. 162) использовать более одного Сервера администрирования. Вы можете выбрать стандартную или выборочную установку Сервера администрирования. Вместе с Сервером администрирования установится Консоль администрирования. Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена.

Стандартная установка (см. стр. 238) рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке вашей сети. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор модулей управления, заданный по умолчанию, для программ "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.

Выборочная установка (см. стр. 243) рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в неинтерактивном режиме (см. стр. 270).

Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования. Можно также выбрать установку Kaspersky Security Center 14.2 Web Console (см. стр. 245).

При необходимости можно установить Консоль администрирования (см. стр. 275) и Kaspersky Security Center 14.2 Web Console на рабочее место администратора независимо для управления Сервером администрирования по сети.

**b. Первоначальная настройка и лицензирование**

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается мастер первоначальной настройки (см. стр. 285). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (см. стр. 83) и задачи (см. стр. 85) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. стр. 400).

Если вы планируете использовать функциональность, выходящую за рамки Базовой функциональности (см. стр. 356), активируйте программу по лицензии. Вы можете выполнить это на одном из шагов (см. стр. 288) мастера первоначальной настройки.

**c. Проверка успешности установки Сервера администрирования**

После успешного выполнения предыдущих шагов Сервер администрирования установлен и готов к дальнейшей работе.

Убедитесь, что работает Консоль администрирования и что вы можете подключиться через Консоль к Серверу администрирования. Убедитесь также, что на Сервере администрирования имеется задача загрузки обновлений в хранилище Сервера администрирования (в папке **Задачи** дерева консоли (см. стр. 890)) и политика для Kaspersky Endpoint Security (в папке **Политики** дерева консоли).

После завершения проверки, перейдите к шагам ниже.

**Удаленное развертывание программ безопасности "Лаборатории Каперского" на клиентских устройствах**

**a. Обнаружение устройств в сети**

Этот шаг входит в мастер первоначальной настройки (см. стр. 299). Вы можете также запустить обнаружение устройств (см. стр. 325) вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

**b. Установка Агента администрирования и программ безопасности на устройства в сети**

Развертывание защиты (см. стр. 400) в сети организации подразумевает установку Агента администрирования и программ безопасности (например, Kaspersky Endpoint Security для Windows) на устройства, которые были обнаружены Сервером администрирования при обнаружении устройств.

Программы безопасности защищают устройства от вирусов и / или других программ, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

При необходимости можно установить Агент администрирования в неинтерактивном (тихом) режиме с файлом ответов (см. стр. 193) или без него (см. стр. 194).

Перед тем как установить Агент администрирования и программы безопасности на устройства в сети, убедитесь, что эти устройства доступны (то есть включены). Вы можете установить Агент администрирования на виртуальные машины, так же как и на физические устройства (см. стр. 201).

Возможна удаленная или локальная установка программ безопасности и Агента администрирования.

Удаленная установка (см. стр. 359) – с помощью мастера развертывания защиты вы можете удаленно установить программу безопасности (например, Kaspersky Endpoint Security для Windows) и Агент администрирования на устройствах, которые были обнаружены Сервером администрирования в сети организации. Как правило, задача удаленной установки успешно развертывает защиту для большинства сетевых устройств. Однако она может возвращать ошибку на некоторых устройствах,

если, например, устройство отключено или недоступно по другой причине. В этом случае рекомендуется вручную подключиться к устройству и использовать локальную установку.

Локальная установка (см. стр. 204) – используется на тех устройствах сети, на которых не удалось развернуть защиту с помощью задачи удаленной установки. Чтобы установить защиту на такие устройства, создайте автономный инсталляционный пакет для запуска на этих устройствах локально.

Установка Агента администрирования на устройства с операционными системами Linux и macOS описана в документации для Kaspersky Endpoint Security для Linux и Kaspersky Endpoint Security для Mac соответственно. Несмотря на то, что устройства под управлением операционных систем Linux и macOS считаются менее уязвимыми, чем устройства под управлением Windows, на них также рекомендуется устанавливать программы безопасности.

После установки убедитесь, что программа безопасности установлена на управляемые устройства. Для этого запустите Отчет о версиях программ "Лаборатории Касперского" и ознакомьтесь с его результатами (см. стр. 569).

**c. Распространение лицензионных ключей на клиентские устройства**

Распространите лицензионные ключи (см. стр. 389) на клиентские устройства, чтобы активировать управляемые программы безопасности на этих устройствах.

**d. Настройка защиты мобильных устройств**

Этот шаг входит в мастер первоначальной настройки.

Чтобы управлять корпоративными мобильными устройствами, выполните необходимые подготовительные шаги и разверните Управление мобильными устройствами.

**e. Создание структуры групп администрирования**

В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования (см. стр. 81) с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам (см. стр. 445) или распределить устройства вручную. Для групп администрирования можно назначать групповые задачи, определять область действия политик и назначать точки распространения.

Убедитесь, что все управляемые устройства правильно распределены по соответствующим группам администрирования и что у вас в сети не осталось нераспределенных устройств (на стр. 325).

**f. Назначение точек распространения**

Kaspersky Security Center автоматически назначает точки распространения (см. стр. 167) группам администрирования, но при необходимости вы можете назначить их вручную. Точки администрирования рекомендуется использовать (см. стр. 658) в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью. В качестве точек распространения можно использовать устройства под управлением Linux (см. стр. 662) и под управлением Windows.

kaspersky

См. также:



# Порты, используемые Kaspersky Security Center

В таблицах ниже перечислены порты, которые должны быть открыты на Серверах администрирования и на клиентских устройствах. Если вы хотите, вы можете изменить номера портов по умолчанию.

В таблице ниже перечислены порты, которые должны быть открыты на Сервере администрирования. Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, порт 1433 для Microsoft SQL Server или порт 5432 для PostgreSQL и Postgres Pro). Подробную информацию см. в документации СУБД.

*Таблица 5. Порты, которые должны быть открыты на Сервере администрирования*

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 8060 | klcsweb | TCP | Передача на клиентские устройства опубликованных инсталляционных пакетов | Публикация инсталляционных пакетов.<br>Вы можете изменить номер порта по умолчанию в разделе **Веб-сервер** (см. стр. 689) окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console. |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 8061 | klcsweb | TCP (TLS) | Передача на клиентские устройства опубликованных инсталляционных пакетов | Публикация инсталляционных пакетов.<br>Вы можете изменить номер порта по умолчанию в разделе **Веб-сервер** (см. стр. 689) окна свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console. |
| 13000 | klserver | TCP (TLS) | Прием подключений от Агентов администрирования и от подчиненных Серверов администрирования; используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне) | Управление клиентскими устройствами и подчиненными Серверами администрирования.<br>Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения (см. стр. 251). Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования в Консоли администрирования (см. стр. 984) или в Kaspersky Security Center 14.2 Web Console (см. стр. 984). |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 13000 | klserver | UDP | Прием информации от Агентов администрирования о выключении устройств | Управление клиентскими устройствами.<br>Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования (см. стр. 750) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1083). |
| 13291 | klserver | TCP (TLS) | Прием подключений от Консоли администрирования к Серверу администрирования | Управление Сервером администрирования.<br>Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (см. стр. 981) в Консоли администрирования. |
| 13299 | klserver | TCP (TLS) | Получение соединений от Kaspersky Security Center 14.2 Web Console к Серверу администрирования; получение соединений от Сервера администрирования через OpenAPI | Kaspersky Security Center 14.2 Web Console, OpenAPI.<br>Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Порты подключения** раздела **Общий**) в Консоли администрирования либо при создании иерархии Серверов администрирования в Консоли администрирования (см. стр. 984) или в Kaspersky Security Center 14.2 Web Console (см. стр. 984). |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 14000 | klserver | TCP | Прием подключений от Агентов администрирования | Управление клиентскими устройствами.<br>Вы можете изменить номер порта по умолчанию при настройке портов подключения (см. стр. 251) при установке Kaspersky Security Center или при подключении клиентского устройства к Серверу администрирования вручную (см. стр. 715). |
| 13111 (только если на устройстве запущена служба прокси-сервера KSN) | ksnproxy | TCP | Прием запросов от управляемых устройств к прокси-серверу KSN | Прокси-сервер KSN.<br>Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. стр. 830). |
| 15111 (только если на устройстве запущена служба прокси-сервера KSN) | ksnproxy | UDP | Прием запросов от управляемых устройств к прокси-серверу KSN | Прокси-сервер KSN.<br>Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. стр. 830). |
| 17000 | klactprx | TCP (TLS) | Прием подключений для активации программ от управляемых устройств (кроме мобильных устройств) | Прокси-сервер активации, используемый немобильными устройствами для активации программ "Лаборатории Касперского" с помощью кодов активации.<br>Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования. |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 17100 (только если вы управляете мобильными устройствами) | klactprx | TCP (TLS) | Прием подключений для активации приложений от мобильных устройств | Прокси-сервер активации для мобильных устройств.<br>Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования. |
| 19170 | klserver | HTTPS (TLS) | Туннелирование соединения (см. стр. 981) с управляемыми устройствами с помощью утилиты klsctunnel | Удаленное подключение к управляемым устройствам с помощью Kaspersky Security Center 14.2 Web Console.<br>Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Дополнительные порты** раздела **Общий**) только в Консоли администрирования. |
| 13292 (только если вы управляете мобильными устройствами) | klserver | TCP (TLS) | Прием подключений от мобильных устройств | Управление мобильными устройствами.<br>Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console. |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 13294 (только если вы управляете мобильными устройствами) | klserver | TCP (TLS) | Прием подключений от устройств с защитой на уровне UEFI | Управление клиентскими устройствами с защитой на уровне UEFI.<br>Вы можете изменить номер порта по умолчанию при подключении мобильных устройств (см. стр. 294) или позже в окне свойств Сервера администрирования (в подразделе Дополнительные порты раздела **Общий**) в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console (см. стр. 983). |

В таблице ниже указан порт, который должен быть открыт на Сервере iOS MDM (только если вы управляете мобильными устройствами).

*Таблица 6. Порт, используемый Сервером iOS MDM*

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 443 | kliosmdmservicesrv | TCP (TLS) | Прием соединений от мобильных устройств iOS | Управление мобильными устройствами.<br>Вы можете изменить номер порта по умолчанию при установке Сервера iOS MDM. |

В таблице ниже указан порт, который должен быть открыт на Сервере Kaspersky Security Center Web Console. Это может быть то же устройство, на котором установлен Сервер администрирования, или другое устройство.

*Таблица 7. Порт, используемый Сервером Kaspersky Security Center Web Console*

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 8080 | Node.js: серверный JavaScript | TCP (TLS) | Прием соединений от браузера и передача в Kaspersky Security Center 14.2 Web Console (см. стр. 950) | Kaspersky Security Center 14.2 Web Console.<br>Вы можете изменить номер порта по умолчанию при установке Kaspersky Security Center 14.2 Web Console на устройстве под управлением Windows (см. стр. 950) или Linux (см. стр. 953). Если вы устанавливаете Kaspersky Security Center 14.2 Web Console на устройство с операционной системой ALT Linux, то необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой. |

В таблице ниже указан порт, который должен быть открыт на управляемых устройствах, на которых установлен Агент администрирования.

*Таблица 8. Порты, используемые Агентом администрирования*

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 15000 | klnagent | UDP | Сигналы управления от Сервера администрирования к Агентам администрирования | Управление клиентскими устройствами.<br>Вы можете изменить номер порта по умолчанию в параметрах политики Агента администрирования в Консоли администрирования (см. стр. 750) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1083). |
| 15000 | klnagent | UDP-трансляция | Получение данных о других Агентах администрирования в том же широковещательном домене (далее данные отправляются на Сервер администрирования) | Доставка обновлений и инсталляционных пакетов. |
| 15001 | klnagent | UDP | Получение многоадресных запросов от точек распространения (если используется) | Получение обновлений и инсталляционных пакетов от точки распространения.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 481) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |

Обратите внимание, что процесс klnagent также может запрашивать свободные порты из динамического диапазона портов операционной системы конечного устройства. Операционная система назначает эти порты процессу klnagent автоматически, поэтому процесс klnagent может использовать некоторые порты, используемые другим программным обеспечением. Если процесс klnagent влияет на работу этого программного обеспечения, измените параметры порта в программном обеспечении или измените динамический диапазон портов по умолчанию в вашей операционной системе, чтобы исключить порт, используемый этим программным обеспечением.

В таблице ниже указаны порты, которые должны быть открыты на управляемом устройстве с установленным Агентом администрирования, выполняющим роль точки распространения. Перечисленные порты должны быть открыты на устройствах, которые выполняют роль точек распространения, в дополнение к портам, используемым Агентами администрирования (см. таблицу выше).

*Таблица 9. Порты, используемые Агентом администрирования, который работает в качестве точки распространения*

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 13000 | klnagent | TCP (TLS) | Прием подключений от Агентов администрирования (см. стр. 1266) | Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 481) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |
| 13111 (только если на устройстве запущена служба прокси-сервера KSN) | ksnproxy | TCP | Прием запросов от управляемых устройств к прокси-серверу KSN | Прокси-сервер KSN.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 481) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |
| 15111 (только если на устройстве запущена служба прокси-сервера KSN) | ksnproxy | UDP | Прием запросов от управляемых устройств к прокси-серверу KSN | Прокси-сервер KSN.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 481) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |

| Номер порта | Имя процесса, открывающего порт | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 17111 (только если на устройстве запущена служба прокси-сервера KSN) | ksnproxy | HTTPS | Прием запросов от управляемых устройств к прокси-серверу KSN | Прокси-сервер KSN.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 481) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |
| 13295 (только если вы используете точку распространения в качестве push-сервера) | klnagent | TCP (TLS) | Отправка push-уведомлений управляемым устройствам | Push-сервер.<br>Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования (см. стр. 668) или в Kaspersky Security Center 14.2 Web Console (см. стр. 1266). |

См. также:

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые программой Kaspersky Security Center 14.2 Web Console ..... 946

Основной сценарий установки ..... 92

# Сертификаты для работы с Kaspersky Security Center

Этот раздел содержит информацию о сертификатах Kaspersky Security Center и описывает, как выпустить пользовательский сертификат для Сервера администрирования.

kaspersky

## В этом разделе



# О сертификатах Kaspersky Security Center

Kaspersky Security Center использует следующие типы сертификатов для обеспечения безопасного взаимодействия между компонентами программы:

- сертификат Сервера администрирования;
- мобильный сертификат;
- сертификат Сервера iOS MDM;
- сертификат Веб-сервера Kaspersky Security Center;
- сертификат Kaspersky Security Center 14.2 Web Console.

По умолчанию Kaspersky Security Center использует самоподписанные сертификаты (то есть выданные самим Kaspersky Security Center). Если требуется, вы можете заменить самоподписанные сертификаты пользовательскими сертификатами, в соответствии со стандартами безопасности вашей организации. После того как Сервер администрирования проверит соответствие пользовательского сертификата всем применимым требованиям, этот сертификат приобретает такую же область действия, что и самоподписанный сертификат. Единственное отличие состоит в том, что пользовательский сертификат не перевыпускается автоматически по истечении срока действия. Вы заменяете сертификаты на пользовательские с помощью утилиты klsetsrvcert (см. стр. 114) или в Консоли администрирования в свойствах Сервера администрирования, в зависимости от типа сертификата. При использовании утилиты klsetsrvcert необходимо указать тип сертификата, используя одно из следующих значений:

- C (общий сертификат для портов 13000 и 13291);
- CR (общий резервный сертификат для портов 13000 и 13291).
- M – мобильный сертификат для порта 13292;
- MR – мобильный резервный сертификат для порта 13292;
- MCA – мобильный сертификат, полученный от аккредитованного центра сертификации для автоматической генерации пользовательских сертификатов.

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Утилита несовместима с предыдущими версиями Kaspersky Security Center.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

**Сертификаты Сервера администрирования**

Сертификат Сервера администрирования необходим для аутентификации Сервера администрирования, а также для безопасного взаимодействия Сервера администрирования и Агента администрирования на управляемых устройствах. При первом подключении Консоли администрирования к Серверу администрирования вам будет предложено подтвердить использование текущего сертификата Сервера администрирования. Такое подтверждение также требуется при каждой замене сертификата Сервера администрирования, после каждой переустановки Сервера администрирования и при подключении подчиненного Сервера администрирования к главному Серверу администрирования. Этот сертификат называется общим ("C").

Также существует общий резервный сертификат ("CR"). Kaspersky Security Center автоматически генерирует этот сертификат за 90 дней до истечения срока действия общего сертификата. Общий резервный сертификат впоследствии используется для замены сертификата Сервера администрирования. Когда истекает срок действия общего сертификата, общий резервный сертификат используется для поддержания связи с экземплярами Агента администрирования, установленными на управляемых устройствах. С этой целью общий резервный сертификат автоматически становится новым общим сертификатом за 24 часа до истечения срока действия старого общего сертификата.

Вы также можете создать резервную копию сертификата Сервера администрирования отдельно от других параметров Сервера администрирования, чтобы перенести Сервер администрирования с одного устройства на другое без потери данных.

**Мобильные сертификаты**

Мобильный сертификат ("M") необходим для аутентификации Сервера администрирования на мобильных устройствах. Вы настраиваете использование мобильного сертификата на шаге мастера первоначальной настройки.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Когда истекает срок действия мобильного сертификата, мобильный резервный сертификат используется для поддержания связи с Агентами администрирования, установленными на управляемых мобильных устройствах. С этой целью мобильный резервный сертификат автоматически становится новым мобильным сертификатом за 24 часа до истечения срока действия старого мобильного сертификата.

Автоматический повторный выпуск мобильных сертификатов не поддерживается. Рекомендуется указать новый мобильный сертификат, когда срок действия существующего истекает. Если срок действия мобильного сертификата истек, а мобильный резервный сертификат не указан, связь между Сервером администрирования и экземплярами Агента администрирования, установленными на управляемых мобильных устройствах, будет потеряна. В этом случае для повторного подключения управляемых мобильных устройств необходимо указать новый мобильный сертификат и переустановить Kaspersky Security для мобильных устройств на каждом управляемом мобильном устройстве.

Если сценарий подключения требует использования сертификата клиента на мобильных устройствах (подключение с двусторонней SSL-аутентификация), вы генерируете эти сертификаты с помощью аккредитованного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, мастер первоначальной настройки позволяет вам начать использовать пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, а интеграция

с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

**Сертификат Сервера iOS MDM**

Сертификат Сервера iOS MDM необходим для аутентификации Сервера администрирования на мобильных устройствах под управлением операционной системы iOS. Взаимодействие с этими устройствами осуществляется через протокол Apple Mobile Device Management (MDM), в котором не используется Агент администрирования. Вместо этого вы устанавливаете специальный iOS MDM-профиль, содержащий клиентский сертификат, на каждом устройстве, чтобы обеспечить двустороннюю SSL-аутентификацию.

Кроме того, мастер первоначальной настройки позволяет вам начать использовать пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, а интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Клиентские сертификаты передаются на устройства iOS, когда вы загружаете эти iOS MDM-профили. Пользовательский сертификат Сервера iOS MDM уникален для каждого управляемого устройства iOS. Вы генерируете все клиентские сертификаты Сервера iOS MDM с помощью аккредитованного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA").

**Сертификат Веб-сервера Kaspersky Security Center**

Специальный тип сертификата использует Веб-сервер Kaspersky Security Center (далее также Веб-сервер) – компонент Сервера администрирования Kaspersky Security Center. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для публикации iOS MDM-профилей, приложений iOS и инсталляционных пакетов Kaspersky Security для мобильных устройств. Для этого Веб-сервер может использовать различные сертификаты.

Если поддержка мобильных устройств отключена, Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли администрирования.
2. Общий сертификат Сервера администрирования ("C").

Если поддержка мобильных устройств включена, Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли администрирования.
2. Пользовательский мобильный сертификат.
3. Самоподписанный мобильный сертификат ("M").
4. Общий сертификат Сервера администрирования ("C").

**Сертификат Kaspersky Security Center 14.2 Web Console**

Сервер Kaspersky Security Center 14.2 Web Console (далее также Web Console) имеет собственный сертификат. Когда вы открываете сайт, браузер проверяет, является ли ваше соединение надежным. Сертификат Web Console позволяет аутентифицировать Web Console и используется для шифрования трафика между браузером и Web Console.

Когда вы открываете Web Console, браузер информирует вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется, так как сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически

генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, вы можете выполнить одно из следующих действий:

- Замените сертификат Kaspersky Security Center Web Console (см. стр. 963) на пользовательский сертификат (рекомендуемый параметр). Создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 112).
- Добавьте сертификат Kaspersky Security Center Web Console в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

### См. также:

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center .....112

Сценарий:Задание пользовательского сертификата Сервера администрирования .....114

Основной сценарий установки.....92

Аутентификация Сервера при подключении Консоли администрирования .....678

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования .....141

Резервное копирование и восстановление данных в интерактивном режиме .....693

Мастер первоначальной настройки Сервера администрирования.....285

Веб-сервер .....79

## О сертификате Сервера администрирования

Выполняются две операции с использованием *сертификата Сервера администрирования*: Аутентификация Сервера администрирования при подключении Консоли администрирования и обмен данными с устройствами. Сертификат используется также для аутентификации, когда главные Серверы администрирования подключены к подчиненным Серверам администрирования.

**Сертификаты, выписанные "Лабораторией Касперского"**

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

Сертификат Сервера администрирования действителен в течение пяти лет, если сертификат выдан до 1 сентября 2020 года. В противном случае срок действия сертификата ограничен 397 днями. Новый сертификат генерируется Сервером администрирования как резервный сертификат, за 90 дней до срока окончания действия текущего сертификата. Затем новый сертификат автоматически замещает текущий сертификат за один день до окончания его срока действия. Все Агенты администрирования на клиентских устройствах автоматически настраиваются на аутентификацию с Сервером администрирования с использованием нового сертификата.

**Пользовательские сертификаты**

При необходимости можно назначить Серверу администрирования пользовательский сертификат. Например, это может понадобиться для лучшей интеграции с существующей PKI вашей организации или для требуемой настройки полей сертификата.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы устранить эту ошибку, вам потребуется восстановить соединение после замены сертификата (см. стр. 114).

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и затем восстановление данных (на стр. 692).

## Требования к пользовательским сертификатам, используемым в Kaspersky Security Center

В таблице ниже представлены требования к пользовательским сертификатам, предъявляемые к различным компонентам Kaspersky Security Center (см. стр. 108).

*Таблица 10. Требования для сертификатов Kaspersky Security Center*

| Тип сертификата | Требования | Комментарии |
|---|---|---|
| Общий сертификат, Общий резервный сертификат ("C", "CR") | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Нет<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента. | Параметр Extended Key Usage является необязательным.<br>Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1. |

| Тип сертификата | Требования | Комментарии |
| --- | --- | --- |
| Мобильный сертификат, Мобильный резервный сертификат ("M", "MR") | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Нет<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (EKU) (необязательно): аутентификация Сервера. | Параметр Extended Key Usage является необязательным.<br>Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. |
| Сертификат, выпущенный аккредитованным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA) | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Нет<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента. | Параметр Extended Key Usage является необязательным.<br>Значение ограничения длины пути может быть целым числом отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1. |

| Тип сертификата | Требования | Комментарии |
|---|---|---|
| Сертификат Веб-сервера | Расширенное использование ключа (EKU): аутентификация Сервера.<br>Контейнер PKCS #12 / PEM, из которого указывается сертификат, включает всю цепочку открытых ключей.<br>Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым.<br>Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum. | Неприменимо. |
| Сертификат Kaspersky Security Center Web Console | Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей.<br>Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым.<br>Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum. | Зашифрованные сертификаты не поддерживаются Kaspersky Security Center Web Console. |

См. также:


О сертификате Сервера администрирования.....111

Сценарий:Задание пользовательского сертификата Сервера администрирования .....114

Основной сценарий установки.....92


## Сценарий: Задание пользовательского сертификата Сервера администрирования

Вы можете назначить пользовательский сертификат Сервера администрирования, например, для лучшей интеграции с существующей инфраструктурой открытых ключей (PKI) вашей организации или для пользовательской конфигурации параметров сертификата. Целесообразно заменять сертификат сразу после инсталляции Сервера администрирования, до завершения работы мастера первоначальной настройки.

Максимальный срок действия любого сертификата Сервера администрирования не должен превышать 397 дней.

**Предварительные требования**

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен аккредитованным центром сертификации (CA). Также новый сертификат должен включать в себя всю цепочку доверия и закрытый ключ, который должен храниться в файле с расширением pfx или p12. Для нового сертификата должны быть соблюдены требования, перечисленные в таблице ниже.

*Таблица 11. Требования к сертификатам Сервера администрирования*

| Тип сертификата | Требования |
|---|---|
| Общий сертификат, общий резервный сертификат ("C", "CR") | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Отсутствует.<br>Значение ограничения длины пути может быть целым числом отличным от "None", но не меньше 1.<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера и аутентификация клиента. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера и клиента должны быть указаны в EKU. |
| Мобильный сертификат, мобильный резервный сертификат ("M", "MR") | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Отсутствует.<br>Значение ограничения длины пути может быть целым числом, отличным от "None", если общий сертификат имеет значение ограничения длины пути не менее 1.<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (EKU): аутентификация Сервера. EKU необязательно, но если оно содержится в вашем сертификате, данные аутентификации Сервера должны быть указаны в EKU. |

| Тип сертификата | Требования |
|---|---|
| Сертификат, выпущенный аккредитованным центром сертификации (CA), для автоматически генерируемых пользовательских сертификатов (MCA) | Минимальная длина ключа: 2048.<br>Основные ограничения:<br>• CA: Да.<br>• Ограничение длины пути: Отсутствует.<br>Значение ограничения длины пути может быть целым числом, отличным от "None", если Общий сертификат имеет значение ограничения длины пути не менее 1.<br>Используемые ключи:<br>• Цифровая подпись.<br>• Подпись сертификата.<br>• Шифрование ключей.<br>• Подписывание списка отзыва (CRL).<br>Расширенное использование ключа (англ. Extended Key Usage, EKU): аутентификация клиента. EKU необязателен, но если он содержится в вашем сертификате, данные аутентификации клиента должны быть указаны в EKU. |

Сертификаты, выпущенные аккредитованным центром сертификации (англ. certificate authority, CA), не имеют разрешения на подписывание сертификатов. Чтобы использовать такие сертификаты, убедитесь, что на точках распространения или шлюзах соединения в вашей сети установлен Агент администрирования версии 13 или выше. В противном случае вы не сможете использовать сертификаты без разрешения на подпись.

**Этапы**

Указание сертификата Сервера администрирования состоит из следующих этапов:

a. **Замена сертификата Сервера администрирования**

   Используйте командную строку утилиты klsetsrvcert (см. стр. 117) для этой цели.

b. **Указание нового сертификата и восстановление связи Агентов администрирования с Сервером администрирования**

   При замене сертификата все Агенты администрирования, ранее подключенные к Серверу администрирования по SSL, перестанут подключаться к Серверу с ошибкой "Ошибка аутентификации Сервера администрирования". Чтобы указать новый сертификат и восстановить соединение, используйте командную строку утилиты klmover (см. стр. 119).

c. **Указание нового сертификата в параметрах Kaspersky Security Center 14.2 Web Console**

   После замены сертификата укажите это (см. стр. 964) в параметрах Kaspersky Security Center 14.2 Web Console. Иначе Kaspersky Security Center 14.2 Web Console не сможет подключиться к Серверу администрирования.

**Результаты**

После завершения сценария сертификат Сервера администрирования будет заменен, Сервер Агент администрирования на управляемых устройствах аутентифицирует Сервер с использованием нового сертификата.

kaspersky

См. также:



## Замена сертификата Сервера администрирования с помощью утилиты klsetsrvcert

► *Чтобы заменить сертификат Сервера администрирования:*

В командной строке выполните следующую команду:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] |
-g <dnsname>}][-f <time>][-r <calistfile>][-l <logfile>]
```

Вам не нужно загружать утилиту klsetsrvcert. Утилита входит в состав комплекта поставки Kaspersky Security Center. Она несовместима с предыдущими версиями Kaspersky Security Center.

Описание параметров утилиты klsetsrvcert представлено в таблице ниже.

*Таблица 12. Значения параметров утилиты klsetsrvcert*

| Параметр | Значение |
|---|---|
| `-t <type>` | Тип сертификата, который следует заменить. Возможные значения параметра `<type>`:<br>• `C` – заменить общий сертификат для портов 13000 и 13291.<br>• `CR` – заменить общий резервный сертификат для портов 13000 и 13291.<br>• `M` – заменить сертификат для мобильных устройств порта 13292.<br>• `MR` – заменить мобильный резервный сертификат для порта 13292.<br>• `MCA` – мобильный сертификат, полученный от аккредитованного центра сертификации для автоматической генерации пользовательских сертификатов. |
| `-f <time>` | Расписание замены сертификата использует формат "ДД-ММ-ГГГГ ЧЧ:ММ" (для портов 13000 и 13291).<br>Используйте этот параметр, если вы хотите заменить общий или общий резервный сертификат до истечения срока его действия.<br>Укажите время, когда управляемые устройства должны синхронизироваться с Сервером администрирования с использованием нового сертификата. |
| `-i <inputfile>` | Контейнер с сертификатом и закрытый ключ в формате PKCS#12 (файл с расширением p12 или pfx). |

| Параметр | Значение |
|---|---|
| `-p <password>` | Пароль, при помощи которого защищен p12-контейнер.<br>Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль. |
| `-o <chkopt>` | Параметры проверки сертификата (разделенные точкой с запятой).<br>Чтобы использовать пользовательский сертификат без разрешения на подпись, в утилите klsetsrvcert укажите `-o NoCA`. Это полезно для сертификатов, выпущенных аккредитованным центром сертификации (англ. certificate authority, CA). |
| `-g <dnsname>` | Сертификат будет создан с указанным DNS-именем. |
| `-r <calistfile>` | Список доверенных корневых сертификатов, подписанных аккредитованным центром сертификации, в формате PEM. |
| `-l <logfile>` | Файл вывода результатов. По умолчанию вывод осуществляется в стандартный поток вывода. |

Например, для указания пользовательского сертификата Сервера администрирования (см. стр. 108), используйте следующую команду:

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

После замены сертификата все Агенты администрирования, подключенные к Серверу администрирования по протоколу SSL, теряют связь. Чтобы восстановить связь, используйте командную строку утилиты klmover (см. стр. 119).

Автоматический повторный выпуск мобильных сертификатов не поддерживается. Рекомендуется указать новый мобильный сертификат, когда срок действия существующего истекает. Если срок действия мобильного сертификата истек, а мобильный резервный сертификат не указан, связь между Сервером администрирования и экземплярами Агента администрирования, установленными на управляемых мобильных устройствах, будет потеряна. В этом случае для повторного подключения управляемых мобильных устройств необходимо указать новый мобильный сертификат и переустановить Kaspersky Security для мобильных устройств на каждом управляемом мобильном устройстве.

Чтобы не потерять соединения Агентов администрирования, используйте следующую команду:

```
klsetsrvcert.exe -f "DD-MM-YYYY hh:mm" -t CR -i <inputfile> -p <password> -
o NoCA
```

где дата `"DD-MM-YYYY hh:mm"` на 3–4 недели раньше текущей. Сдвиг времени замены сертификата на резервный позволит распространить новый сертификат на все Агенты администрирования.

## См. также:

Сценарий:Задание пользовательского сертификата Сервера администрирования .....114

kaspersky

# Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

После замены сертификата Сервера администрирования с помощью командной строки утилиты klsetsrvcert (см. стр. 117) вам необходимо установить SSL-соединение между Агентами администрирования и Сервером администрирования, так как соединение разорвано.

► *Чтобы указать новый сертификат Агента администрирования и восстановить соединение:*

В командной строке выполните следующую команду:

```
Klmover [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>]
```

Для запуска утилиты требуются права администратора.

Эта утилита автоматически копируется в папку установки Агента администрирования при установке Агента администрирования на клиентское устройство.

Описание параметров утилиты klmover представлено в таблице ниже.

*Таблица 13. Значения параметров утилиты klmover*

| Параметр | Значение |
|---|---|
| `-address <адрес Сервера>` | Адрес Сервера администрирования для подключения.<br>В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя. |
| `-pn <номер порта>` | Номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования.<br>По умолчанию установлен порт 14000. |
| `-ps <номер SSL-порта>` | Номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL.<br>По умолчанию установлен порт 13000. |
| `-nossl` | Использовать незашифрованное подключение к Серверу администрирования.<br>Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу. |
| `-cert <путь к файлу сертификата>` | Использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования. |
| `-virtserv` | Имя виртуального Сервера администрирования. |

| Параметр | Значение |
|---|---|
| `-cloningmode` | Режим клонирования диска Агента администрирования.<br>Используйте один из следующих параметров для настройки режима клонирования диска:<br>• `-cloningmode` – запрос состояния режима клонирования диска.<br>• `-cloningmode 1` – включить режим клонирования диска.<br>• `-cloningmode 0` – выключить режим клонирования диска. |

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

### См. также:

Сценарий:Задание пользовательского сертификата Сервера администрирования .....114

Подключение клиентского устройства к Серверу администрирования вручную.Утилита klmover ...715

## Перевыпуск сертификата Веб-сервера

Сертификат Веб-сервера используемый в Kaspersky Security Center необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для публикации iOS MDM-профилей, приложений для iOS и инсталляционных пакетов Kaspersky Security для мобильных устройств. В зависимости от текущей конфигурации программы в качестве сертификата Веб-сервера могут использоваться различные сертификаты (подробнее см. О сертификатах Kaspersky Security Center (на стр. 108)).

Вам может потребоваться перевыпустить сертификат Веб-сервера, чтобы обеспечить соответствие требованиям безопасности вашей организации или для поддержания постоянного соединения ваших управляемых устройств перед началом обновления программы (на стр. 281). Kaspersky Security Center предоставляет два способа перевыпуска сертификата Веб-сервера. Выбор между двумя способами зависит от того, подключены ли у вас мобильные устройства и управляются ли они через мобильный протокол (то есть с помощью мобильного сертификата).

Если вы никогда не указывали пользовательский сертификат в качестве сертификата Веб-сервера в окне **Веб-сервер** свойств Сервера администрирования, мобильный сертификат действует как сертификат Веб-сервера. В этом случае перевыпуск сертификата Веб-сервера выполняется путем перевыпуска самого мобильного протокола.

► *Чтобы перевыпустить сертификат Веб-сервера, когда у вас нет мобильных устройств, управляемых через мобильный протокол:*

1. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервер администрирования выберите раздел **Свойства подключения Сервера администрирования**.
3. В списке подразделов выберите подраздел **Сертификаты**.

4. Если вы планируете и дальше использовать сертификат, выданный Kaspersky Security Center, выполните следующие действия:

   a. В группе параметров **Аутентификация Сервера администрирования мобильными устройствами** выберите параметр **Сертификат выпущен средствами Сервера администрирования** и нажмите на кнопку **Перевыпустить**.

   b. В открывшемся окне **Перевыпуск сертификата** в группе параметров **Адрес подключения** и **Срок активации** выберите соответствующие параметры и нажмите на кнопку **ОК**.

   c. В появившемся окне нажмите на кнопку **Да**.

   Если вы планируете использовать собственный сертификат, выполните следующее:

   d. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center (на стр. 112) и требованиям к доверенным сертификатам Apple https://support.apple.com/en-us/HT210176. При необходимости измените сертификат.

   e. Выберите параметр **Другой сертификат** и нажмите на кнопку **Обзор**.

   f. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата и укажите расположение сертификата и параметры:

      - Если вы выбрали **Контейнер PKCS #12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если установлен)**.
      - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если установлен)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

   g. В окне **Сертификат** нажмите на кнопку **ОК**.

   h. В появившемся окне нажмите на кнопку **Да**.

   Мобильный сертификат перевыпущен для использования в качестве сертификата Веб-сервера.

► *Чтобы перевыпустить сертификат Веб-сервера, когда у вас есть мобильные устройства, управляемые через мобильный протокол:*

1. Создайте пользовательский сертификат и подготовьте его для использования в Kaspersky Security Center. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center (на стр. 112)и требованиям к доверенным сертификатам Apple https://support.apple.com/en-us/HT210176. При необходимости измените сертификат.

   Для создания сертификата можно использовать утилиту kliossrvcertgen.exehttps://support.kaspersky.com/10890#block1.

2. В дереве консоли, в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервер администрирования выберите раздел **Веб-сервер**.
4. В меню **По протоколу HTTPS** выберите параметр **Задать другой сертификат**.
5. В меню **По протоколу HTTPS** нажмите на кнопку **Изменить**.
6. В открывшемся окне **Сертификат** в поле **Тип сертификата** выберите тип вашего сертификата:

- Если вы выбрали **Контейнер PKCS #12**, нажмите на кнопку **Обзор** рядом с полем **Файл сертификата** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если установлен)**.
- Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ (.prk, .pem)** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если установлен)**. Нажмите на кнопку **Обзор** рядом с полем **Открытый ключ (.cer)** и укажите закрытый ключ на жестком диске.

7. В окне **Сертификат** нажмите на кнопку **ОК**.
8. При необходимости в окне свойств Сервера администрирования в поле **HTTPS-порт Веб-сервера** измените номер HTTPS-порта для Веб-сервера. Нажмите на кнопку **ОК**.

   Сертификат Веб-сервера перевыпущен.

# Схемы трафика данных и использования портов

В этом разделе приведены схемы трафика данных между компонентами Kaspersky Security Center, управляемыми программами безопасности и внешними серверами для различных конфигураций. Схемы содержат номера портов, которые должны быть доступны на локальных устройствах.

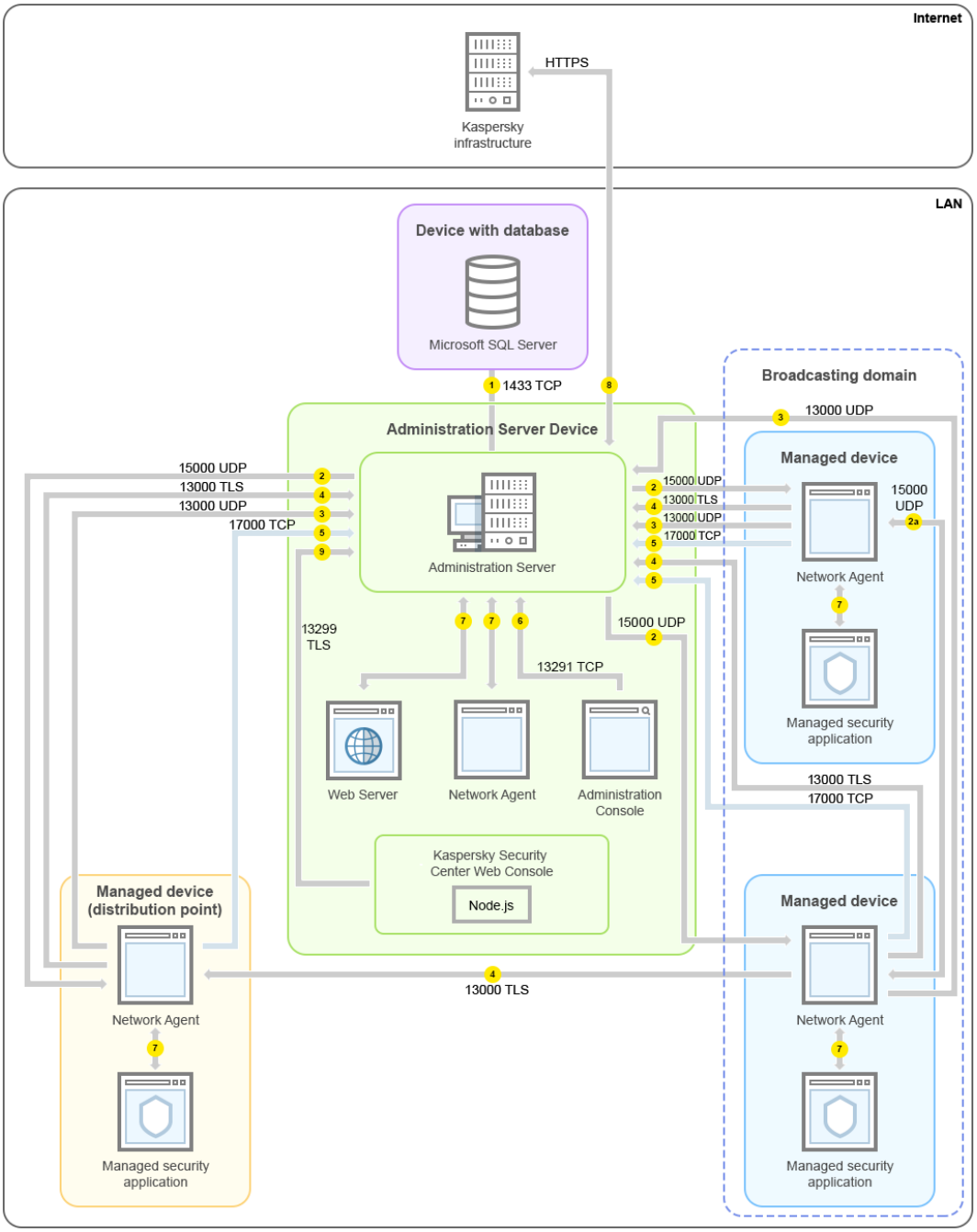
## См. также:

Основной сценарий установки ..... 92

## В этом разделе

# Сервер администрирования и управляемые устройства в локальной сети (LAN)

На рисунке ниже показан трафик данных, если Kaspersky Security Center развернут только в локальной сети (LAN).




На рисунке показано как разные управляемые устройства подключаются к Серверу администрирования различными способами: напрямую или с помощью точки распространения. Точки распространения уменьшают нагрузку на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Однако точки распространения нужны только в том случае, если количество управляемых устройств достаточно велико (см. стр. 167). Если количество управляемых устройств мало, все управляемые устройства могут получать обновления непосредственно с Сервера администрирования.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. стр. 138). Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. стр. 139).

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 139) и от подчиненных Серверов администрирования (см. стр. 141) через SSL-порт 13000.

   Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по незащищенному порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.
5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. стр. 138). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Программы на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления программ и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.
9. Сервер Kaspersky Security Center Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299 (см. стр. 145).

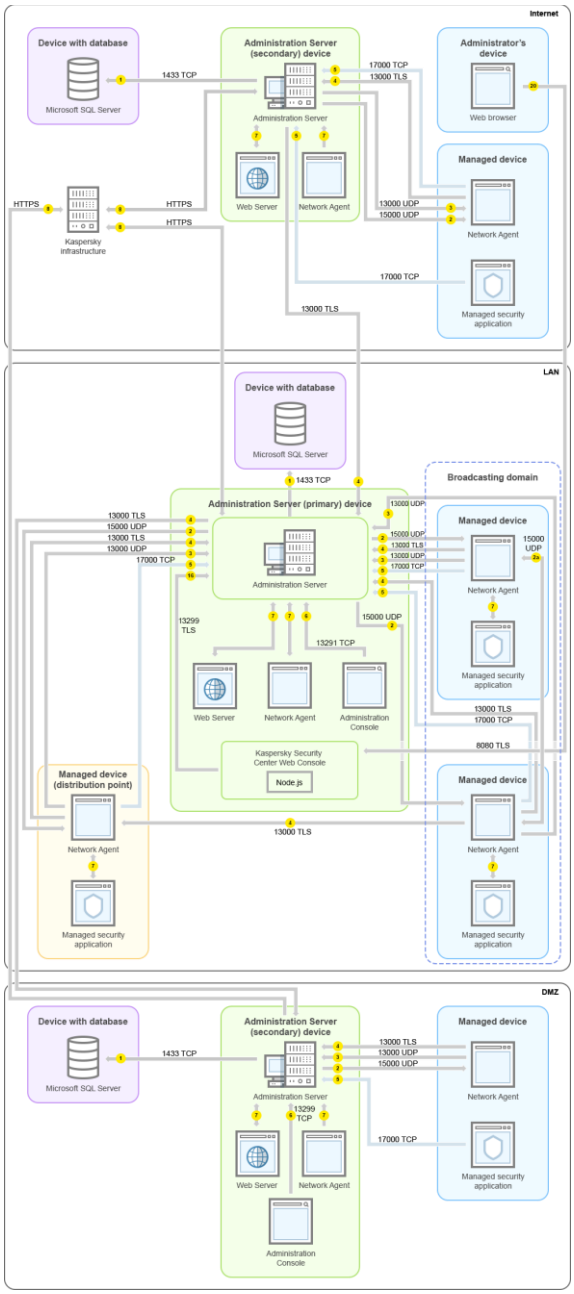
kaspersky

См. также:



## Главный Сервер администрирования в локальной сети (LAN) и два подчиненных Сервера администрирования

На рисунке показана иерархия Серверов администрирования: главный Сервер администрирования расположен внутри локальной сети (LAN). Подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ); другой подчиненный Сервер администрирования расположен в интернете.



Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. стр. 138). Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. стр. 139).

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 139) и от подчиненных Серверов администрирования (см. стр. 141) через SSL-порт 13000.

   Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по незащищенному порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.
5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. стр. 138). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Программы на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления программ и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.
9. Сервер Kaspersky Security Center 14.2 Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center 14.2 Web Console через TLS-порт 8080 (см. стр. 145). Сервер

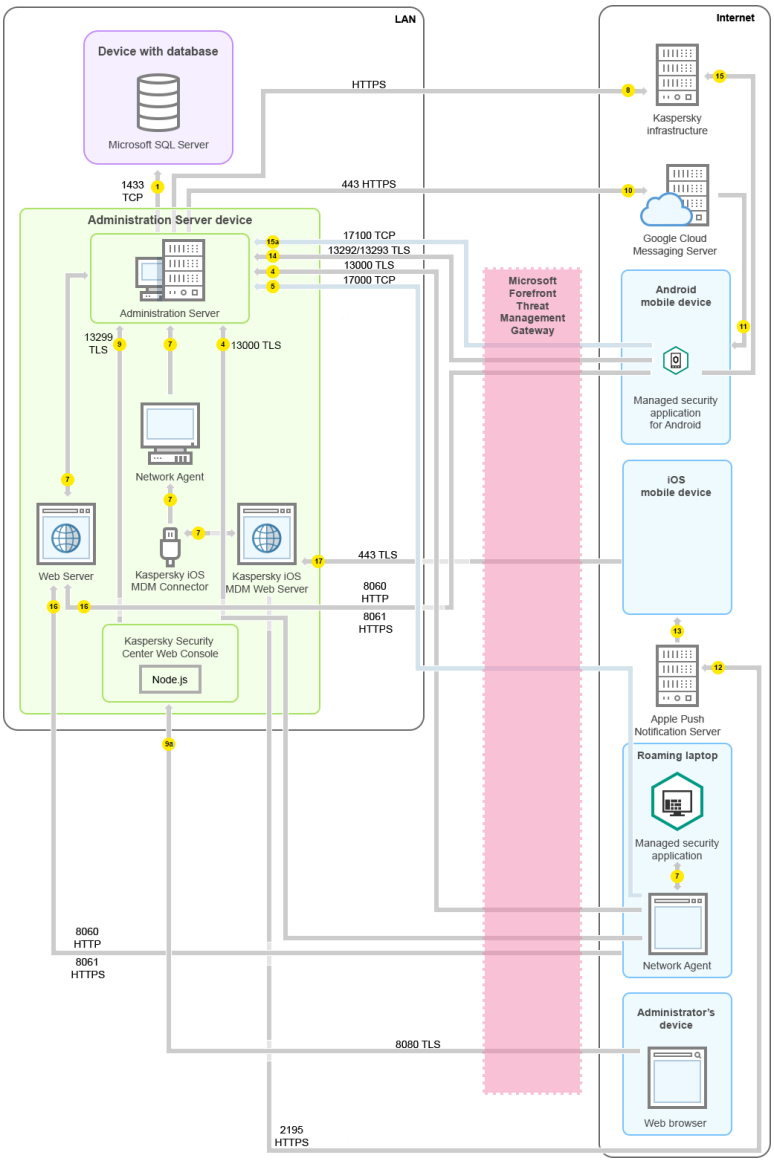
Kaspersky Security Center 14.2 Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

См. также:



## Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование TMG

На рисунке ниже показан трафик данных, когда Сервер администрирования находится внутри локальной сети (LAN), а управляемые устройства, включая мобильные устройства, находятся в интернете. На этом рисунке используется *Microsoft Forefront Threat Management Gateway* (TMG). Однако, если вы хотите использовать корпоративный сетевой экран, вы можете использовать другую программу; дополнительную информацию см. в документации к программе.



Эта схема развертывания рекомендуется, если вы не хотите, чтобы мобильные устройства подключались напрямую к Серверу администрирования, и не хотите назначать шлюз соединения в демилитаризованной зоне (DMZ).

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. стр. 138). Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. стр. 139).

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 139) и от подчиненных Серверов администрирования (см. стр. 141) через SSL-порт 13000.

   Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по незащищенному порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.
5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. стр. 138). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Программы на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления программ и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.

9. Сервер Kaspersky Security Center 14.2 Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center 14.2 Web Console через TLS-порт 8080 (см. стр. 145). Сервер Kaspersky Security Center 14.2 Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.

11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.

12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.

13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.

14. Только для мобильных устройств: управляемая программа передает данные на Сервер администрирования через TLS-порт 13292 / 13293 (см. стр. 146) напрямую, или через Microsoft Forefront Threat Management Gateway (TMG).

15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

    15a. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. стр. 146), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.

16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 79), который находится на том же устройстве, на котором установлен Сервер администрирования.

17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

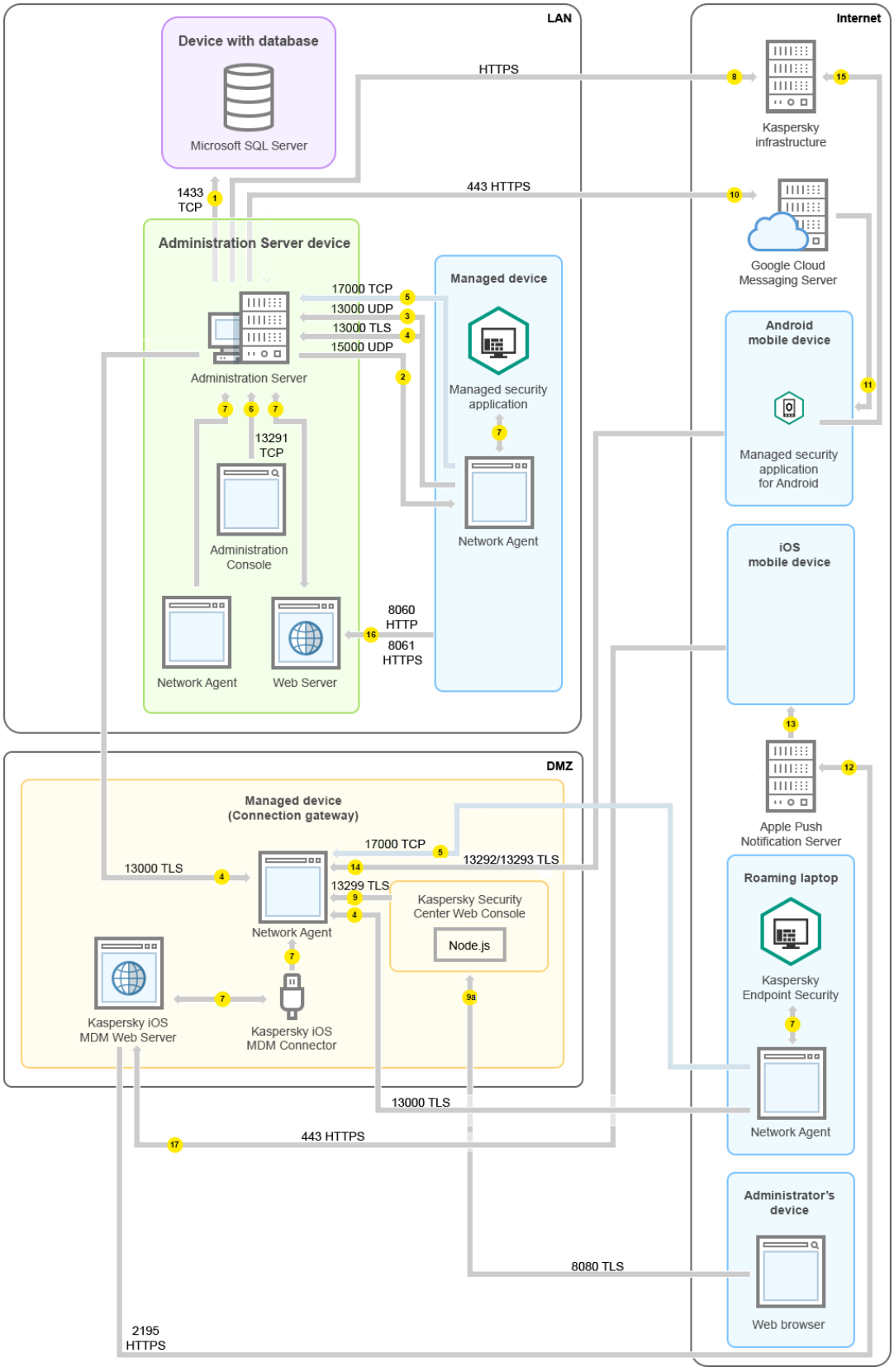
### См. также:

Порты, используемые Kaspersky Security Center.....98

## Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения

На рисунке ниже показан трафик данных, когда Сервер администрирования находится внутри локальной сети (LAN), а управляемые устройства, включая мобильные устройства, находятся в интернете. Шлюз соединения используется.

Эта схема развертывания рекомендуется, если вы не хотите, чтобы мобильные устройства подключались непосредственно к Серверу администрирования, и не хотите использовать Microsoft Forefront Threat Management Gateway (TMG) или корпоративный сетевой экран.



На этом рисунке управляемые устройства подключены к Серверу администрирования через шлюз соединений, который расположен в демилитаризованной зоне (DMZ). TMG или корпоративный сетевой экран не используются.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. стр. 138). Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. стр. 139).

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 139) и от подчиненных Серверов администрирования (см. стр. 141) через SSL-порт 13000.

   Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по незащищенному порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.
5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. стр. 138). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Программы на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу администрирования (например, обновления программ и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.

9. Сервер Kaspersky Security Center 14.2 Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center 14.2 Web Console через TLS-порт 8080 (см. стр. 145). Сервер Kaspersky Security Center 14.2 Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.

11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.

12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.

13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.

14. Только для мобильных устройств: управляемая программа передает данные на Сервер администрирования через TLS-порт 13292 / 13293 (см. стр. 146) напрямую, или через Microsoft Forefront Threat Management Gateway (TMG).

15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

    15a. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. стр. 146), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.

16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 79), который находится на том же устройстве, на котором установлен Сервер администрирования.

17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

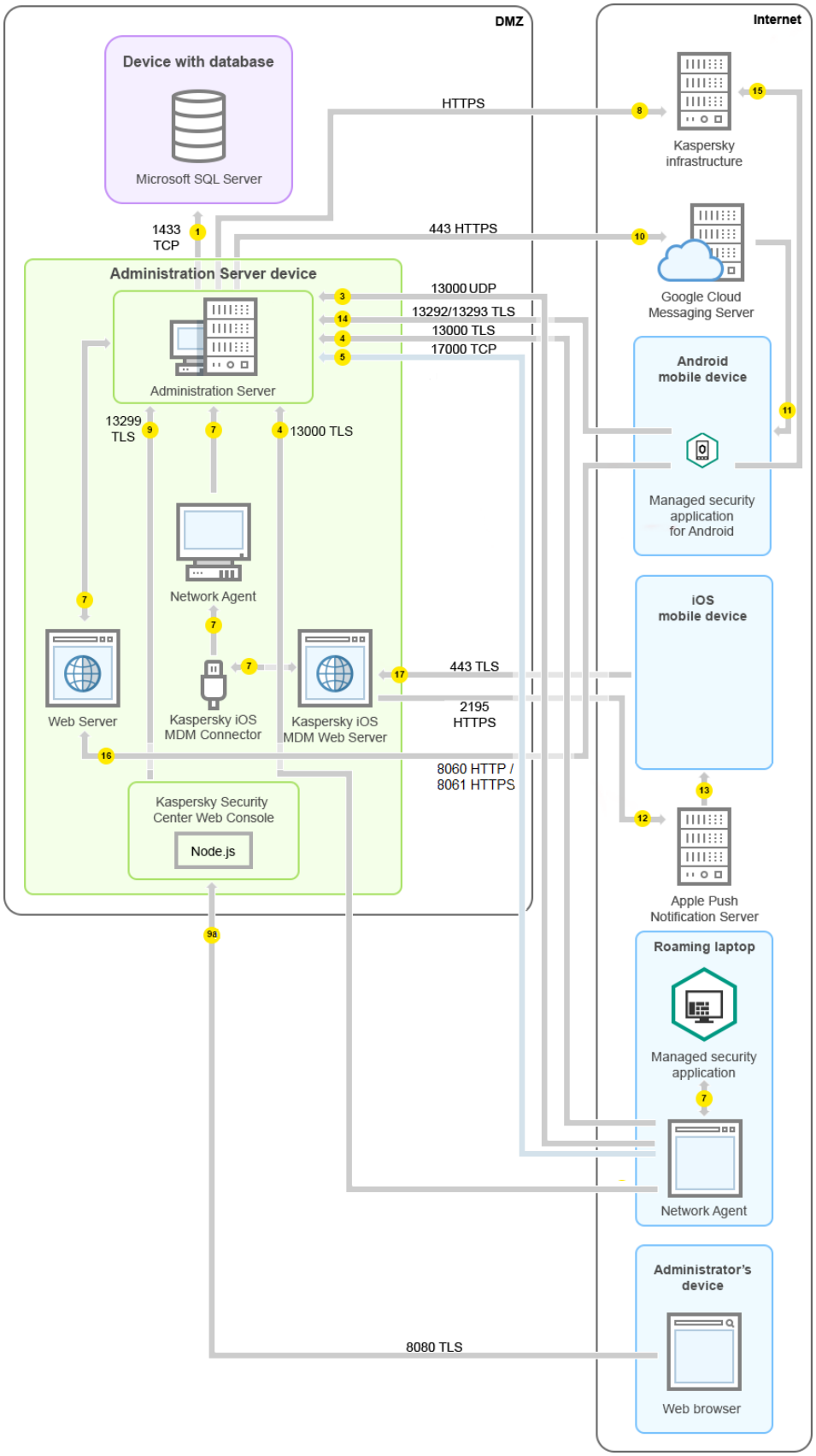
### См. также:

Порты, используемые Kaspersky Security Center.....98

Об использовании точки распространения в качестве шлюза соединений.....667

## Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете

На рисунке ниже показан трафик данных, когда Сервер администрирования расположен в демилитаризованной зоне, а управляемые устройства расположены в интернете, включая мобильные устройства.




На этом рисунке шлюз соединения не используется: мобильные устройства подключаются к Серверу администрирования напрямую.

Стрелки указывают направление трафика: каждая стрелка проведена от устройства, которое инициирует соединение, к устройству, которое "отвечает" на вызов. Указаны номер порта и название протокола, используемые для передачи данных. Каждая стрелка пронумерована и содержит следующую информацию о соответствующем трафике данных:

1. Сервер администрирования передает данные в базу данных (см. стр. 138). Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000 (см. стр. 139).

   Агенты администрирования отправляют запросы друг другу в пределах одного широковещательного домена. Затем данные отправляются на Сервер администрирования и используются для определения пределов широковещательного домена и для автоматического назначения точек распространения (если этот параметр включен).
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 139) и от подчиненных Серверов администрирования (см. стр. 141) через SSL-порт 13000.

   Если вы используете Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключение от Агентов администрирования по незащищенному порту 14000. Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.

   > Точка распространения в ранних версиях Kaspersky Security Center называлась агентом обновлений.

   4a. Шлюз соединений (см. стр. 90) в демилитаризованной зоне также принимает подключение от Сервера администрирования по SSL-порту 13000 (см. стр. 144). Так как шлюз соединения в демилитаризованной зоне не может получить доступ к портам Сервера администрирования, Сервер администрирования создает и поддерживает постоянное сигнальное соединение со шлюзом соединения. Сигнальное соединение не используется для передачи данных; оно используется только для отправки приглашения к сетевому взаимодействию. Когда шлюзу соединения необходимо подключиться к Серверу, он уведомляет Сервер через это сигнальное соединение, а затем Сервер создает необходимое соединение для передачи данных.

   Внешние устройства также подключаются к шлюзу соединения через SSL-порт 13000 (см. стр. 144).
5. Управляемые устройства (кроме мобильных устройств) запрашивают активацию через TCP-порт 17000. В этом нет необходимости, если устройство имеет собственный доступ в интернет; в этом случае устройство отправляет данные на серверы "Лаборатории Касперского" напрямую через интернет.
6. Данные от Консоли администрирования на основе консоли Microsoft Management Console передаются на Сервер администрирования через порт 13291 (см. стр. 138). Консоль администрирования может быть установлена на том же устройстве или на другом.
7. Программы на одном устройстве обмениваются локальным трафиком (либо на Сервере администрирования, либо на управляемом устройстве). Открывать внешние порты не требуется.
8. Данные от Сервера администрирования к серверам "Лаборатории Касперского" (например, данные KSN, информация о лицензиях) и данные от серверов "Лаборатории Касперского" к Серверу

администрирования (например, обновления программ и обновления антивирусных баз) передаются по протоколу HTTPS.

Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.

9. Сервер Kaspersky Security Center 14.2 Web Console передает данные на Сервер администрирования, который может быть установлен на том же устройстве или на другом, через TLS-порт 13299.

   9a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center 14.2 Web Console через TLS-порт 8080 (см. стр. 145). Сервер Kaspersky Security Center 14.2 Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

10. Только для мобильных устройств Android: данные от Сервера администрирования передаются службам Google. Это соединение используется для уведомления мобильных устройств Android о том, что требуется их подключение к Серверу администрирования. Затем push-уведомления отправляются на мобильные устройства.

11. Только для мобильных устройств Android: push-уведомления от серверов Google отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств о том, что требуется их подключение к Серверу администрирования.

12. Только для мобильных устройств iOS: данные от Сервера iOS MDM передаются на серверы Apple Push Notification. Затем push-уведомления отправляются на мобильные устройства.

13. Только для мобильных устройств iOS: push-уведомления от серверов Apple отправляются к мобильному устройству. Это соединение используется для уведомления мобильных устройств iOS о том, что требуется их подключение к Серверу администрирования.

14. Только для мобильных устройств: управляемая программа передает данные на Сервер администрирования через TLS-порт 13292 / 13293 (см. стр. 146) напрямую, или через Microsoft Forefront Threat Management Gateway (TMG).

15. Только для мобильных устройств: данные от мобильного устройства передаются к инфраструктуре "Лаборатории Касперского".

    15a. Если мобильное устройство не имеет доступа в интернет, данные передаются на Сервер администрирования через порт 17100 (см. стр. 146), а Сервер администрирования передает их инфраструктуре "Лаборатории Касперского". Однако этот сценарий используется очень редко.

16. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 79), который находится на том же устройстве, на котором установлен Сервер администрирования.

17. Только для мобильных устройств iOS: данные от мобильных устройств передаются по TLS-порту 443 на Сервер iOS MDM, который находится на том же устройстве, на котором установлен Сервер администрирования или шлюз соединения.

## См. также:

Порты, используемые Kaspersky Security Center.....98

# Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения

В этом разделе приведены схемы взаимодействия между компонентами в составе Kaspersky Security Center и управляемыми программами безопасности. На схемах приведены номера портов, которые должны быть доступны, и имена процессов, открывающих порты.

## См. также:

Основной сценарий установки ..... 92

## В этом разделе



## Условные обозначения в схемах взаимодействия

В таблице ниже приведены условные обозначения, использованные в схемах.

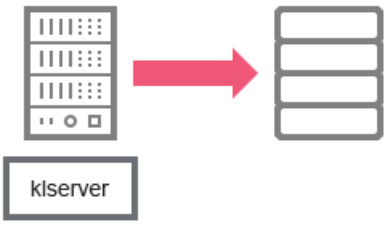
*Таблица 14. Условные обозначения*

| Иконка | Значение |
|---|---|
|  | Сервер администрирования |
|  | Главный Сервер администрирования |

| Иконка | Значение |
| --- | --- |
|  | СУБД |
|  | Клиентское устройство, на котором установлены Агент администрирования и программа семейства Kaspersky Endpoint Security (либо другая программа безопасности, которой может управлять Kaspersky Security Center) |
|  | Шлюз соединения |
|  | Точка распространения |
|  | Мобильное клиентское устройство с установленной программой Kaspersky Security для мобильных устройств |
|  | Браузер на устройстве пользователя |
|   | Процесс, запущенный на устройстве и открывающий какой-либо порт |
|   | Порт и его номер |
|  | Трафик TCP (направление стрелки обозначает направление трафика) |
|  | Трафик UDP (направление стрелки обозначает направление трафика) |
|  | Вызов COM |
|  | Транспорт СУБД |
|  | Границы демилитаризованной зоны |

## Сервер администрирования и СУБД

Данные от Сервера администрирования поступают в базу данных SQL Server, MySQL, MariaDB, PostgreSQL или Postgres Pro.




Если вы установили Сервер администрирования и базу данных на разные устройства, вы должны сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MySQL Server и MariaDB Server, или порт 1433 для Microsoft SQL Server). Подробную информацию см. в документации СУБД.

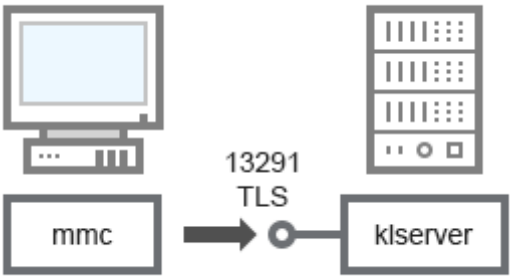
### См. также:

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

## Сервер администрирования и Консоль администрирования




Пояснения к схеме см. в таблице ниже.

*Таблица 15. Сервер администрирования и Консоль администрирования (трафик)*

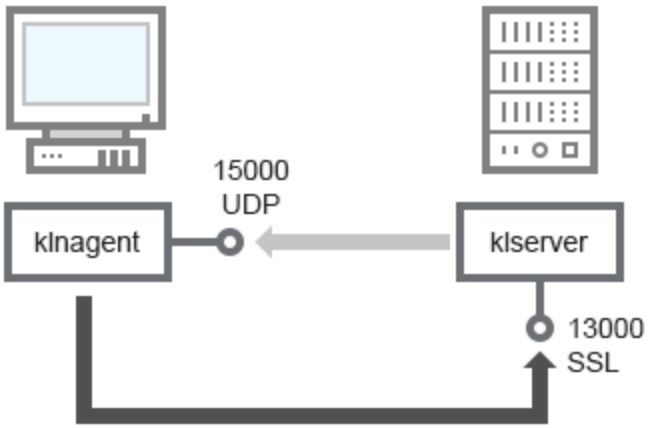
| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Сервер администрирования | 13291 | klserver | TCP | Да | Прием подключений от Консоли администрирования |

См. также:

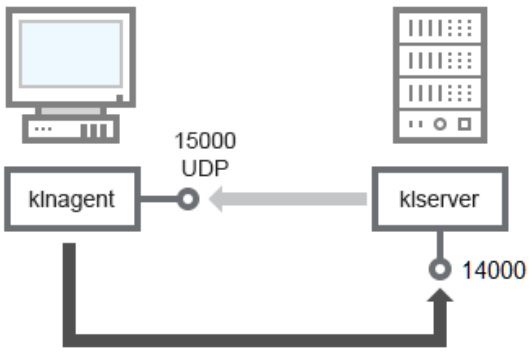


## Сервера администрирования и клиентское устройство: управление программой безопасности

Сервер администрирования принимает подключения от Агентов администрирования по защищенному порту 13000 (см. рис. ниже).




Если вы использовали Kaspersky Security Center одной из предыдущих версий, то в вашей сети Сервер администрирования может принимать подключения от Агентов администрирования по незащищенному порту 14000 (см. рис. ниже). Kaspersky Security Center также поддерживает подключение Агентов администрирования по порту 14000, однако рекомендуется использовать защищенный порт 13000.




Пояснения к схемам см. в таблице ниже.

*Таблица 16. Сервер администрирования и клиентское устройство: Управление программой безопасности (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS (только для TCP) | Назначение порта |
|---|---|---|---|---|---|
| Агент администрирования | 15000 | klnagent | UDP | Нет значения | Многоадресная рассылка Агентам администрирования |
| Сервер администрирования | 13000 | klserver | TCP | Да | Прием подключений от Агентов администрирования |
| Сервер администрирования | 14000 | klserver | TCP | Нет | Прием подключений от Агентов администрирования |

См. также:

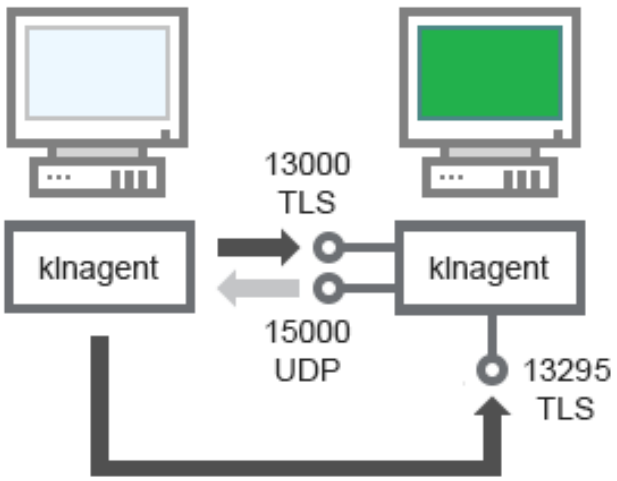
Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

## Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

Клиентское устройство подключается к точке распространения через порт 13000 и, если вы используете точку распространения в качестве push-сервера (см. стр. 668), также через порт 13295; точка распространения выполняет многоадресную рассылку Агентам администрирования через порт 15000 (см. рисунок ниже).



Пояснения к схеме см. в таблице ниже.

*Таблица 17. Обновление программного обеспечения с помощью точки распространения (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS (только для TCP) | Назначение порта |
|---|---|---|---|---|---|
| Агент администрирования | 15000 | klnagent | UDP | Нет значения | Многоадресная рассылка Агентам администрирования |
| Точка распространения | 13000 | klnagent | TCP | Да | Прием подключений от Агентов администрирования |
| Точка распространения | 13295 | klnagent | TCP | Да | Отправка push-уведомлений Агенту администрирования |

## См. также:


Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

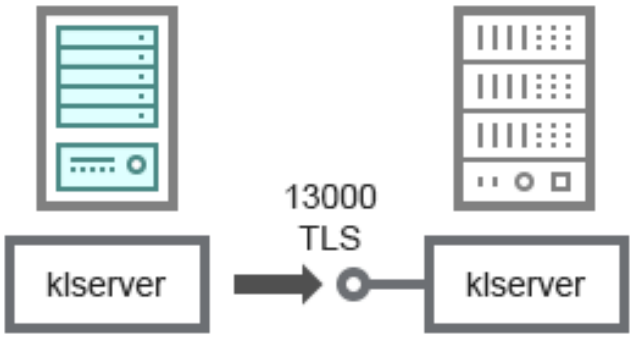
Порты, используемые Kaspersky Security Center ..... 98


## Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

На схеме (см. рис. ниже) показано, как используется порт 13000 для взаимодействия Серверов администрирования, объединенных в иерархию.

При объединении Серверов в иерархию (см. стр. 671) необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. стр. 138).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.



Пояснения к схеме см. в таблице ниже.

*Таблица 18. Иерархия Серверов администрирования (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Главный Сервер администрирования | 13000 | klserver | TCP | Да | Прием подключений от подчиненных Серверов администрирования |

## См. также:

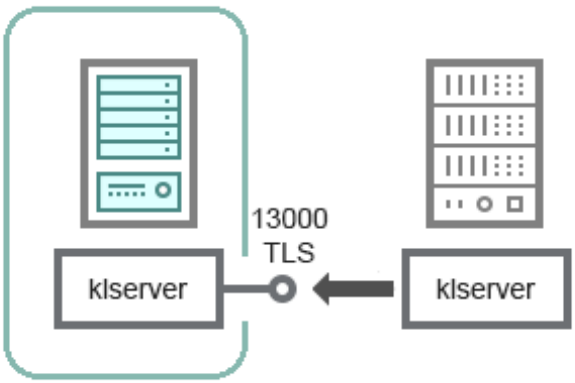

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования ..... 671


## Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне




На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию (см. стр. 671) необходимо, чтобы порт 13291 обоих Серверов был доступен. Через порт 13291 происходит подключение Консоли администрирования к Серверу администрирования (см. стр. 138).

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Консоль администрирования, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13291 главного Сервера был доступен.

Таблица 19. Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне (трафик)

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Главный Сервер администрирования | 13000 | klserver | TCP | Да | Прием подключений от главного Сервера администрирования |

## См. также:


Условные обозначения в схемах взаимодействия ..... 136

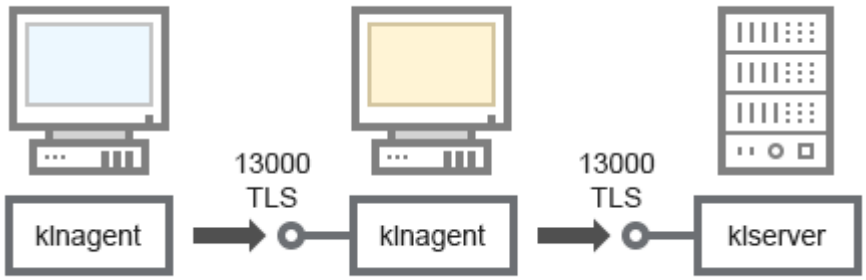
Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

Настройка подключения Консоли администрирования к Серверу администрирования ..... 300

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования ..... 671


## Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство




Пояснения к схеме см. в таблице ниже.

Таблица 20. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Сервер администрирования | 13000 | klserver | TCP | Да | Прием подключений от Агентов администрирования |
| Агент администрирования | 13000 | klnagent | TCP | Да | Прием подключений от Агентов администрирования |

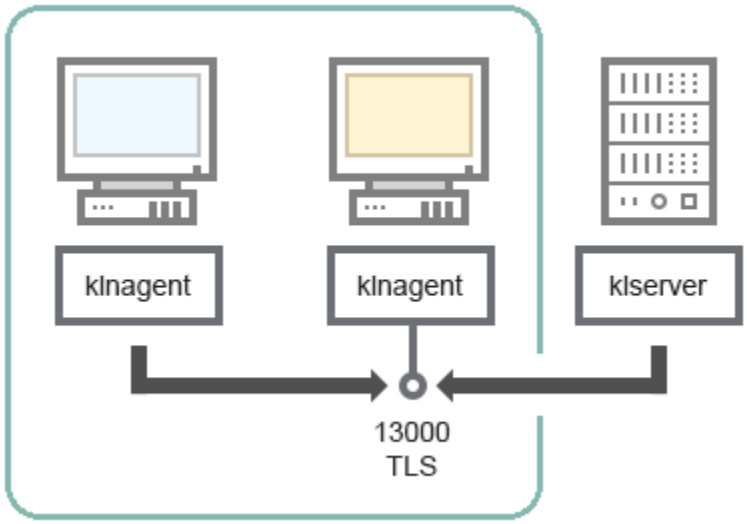
## См. также:

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

## Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство




Пояснения к схеме см. в таблице ниже.

*Таблица 21. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Агент администрирования | 13000 | klnagent | TCP | Да | Прием подключений от Агентов администрирования |

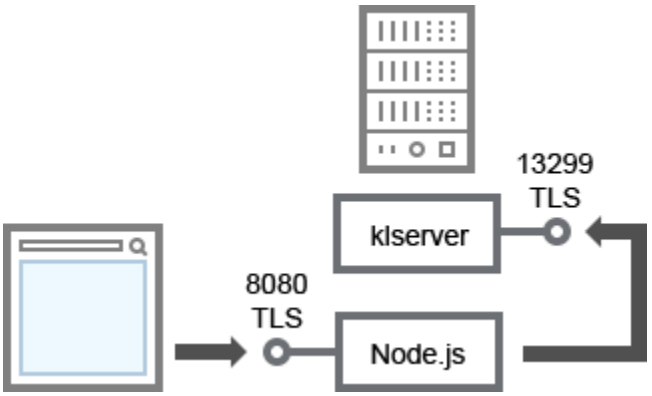
## См. также:

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

## Сервер администрирования и Kaspersky Security Center 14.2 Web Console




Пояснения к схеме см. в таблице ниже.

*Таблица 22. Сервер администрирования и Kaspersky Security Center 14.2 Web Console (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Сервер администрирования | 13299 | klserver | TCP | Да | Получение соединений от Kaspersky Security Center 14.2 Web Console к Серверу администрирования через OpenAPI |
| Сервер Kaspersky Security Center 14.2 Web Console или Сервер администрирования | 8080 | Node.js: серверный JavaScript | TCP | Да | Получение соединений от Kaspersky Security Center 14.2 Web Console |

Kaspersky Security Center 14.2 Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

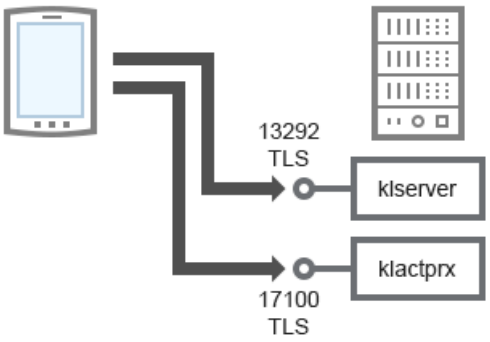
### См. также:

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

### Активация и управление приложением безопасности на мобильном устройстве




Пояснения к схеме см. в таблице ниже.

*Таблица 23. Активация и управление приложением безопасности на мобильном устройстве (трафик)*

| Устройство | Номер порта | Имя процесса, открывающего порт | Протокол | TLS | Назначение порта |
|---|---|---|---|---|---|
| Сервер администрирования | 13292 | klserver | TCP | Да | Прием подключений от Консоли администрирования к Серверу администрирования |
| Сервер администрирования | 17100 | klactprx | TCP | Да | Прием подключений для активации приложений от мобильных устройств |

См. также:

Условные обозначения в схемах взаимодействия ..... 136

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

Порты, используемые Kaspersky Security Center ..... 98

# Лучшие практики развертывания

Kaspersky Security Center является распределенной программой. В состав Kaspersky Security Center входят следующие программы:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Консоль администрирования – основной инструмент администратора. Консоль администрирования поставляется вместе с Сервером администрирования, но может быть также установлена отдельно на одно или несколько устройств администратора.
- Агент администрирования – служит для управления установленной на устройстве программой безопасности, а также для получения информации об устройстве и передаче этой информации на

Сервер администрирования. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Консоли администрирования на устройстве администратора;
- установка Агента администрирования и программы безопасности на устройства организации.

### В этом разделе



# Руководство по усилению защиты

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации. Kaspersky Security Center позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".

Сервер администрирования Kaspersky Security Center имеет полный доступ к управлению защитой клиентских устройств и является важнейшим компонентом системы защиты организации. Поэтому для Сервера администрирования требуются усиленные меры защиты.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;
- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы.

kaspersky

## В этом разделе



# Развертывание Сервера администрирования

### Архитектура Сервера администрирования

В общем случае на выбор архитектуры централизованного управления влияют расположение защищаемых устройств, доступы из смежных сетей, схемы обновления баз и другие параметры.

На начальном этапе проработки архитектуры мы рекомендуем ознакомиться с компонентами Kaspersky Security Center (см. стр. 91) и их взаимодействием между собой, а также со схемами трафика данных и использования портов (см. стр. 122).

На основании этой информации нужно сформировать архитектуру, определяющую:

- расположение Сервера администрирования и подключение к сети;
- организацию рабочих мест администраторов и способы подключения к Серверу администрирования;
- способ установки Агента администрирования и программы безопасности;
- использование точек распространения;
- использование виртуальных Серверов администрирования;
- использование иерархии Серверов администрирования;
- схему обновления антивирусных баз;
- другие информационные потоки.

### Выбор устройства для Сервера администрирования

Сервер администрирования рекомендуется устанавливать на выделенный сервер в инфраструктуре. Если на сервере отсутствует стороннее программное обеспечение, это позволит настроить параметры безопасности с учетом требований Kaspersky Security Center и без зависимости от требований стороннего программного обеспечения.

Сервер администрирования может быть развернут как на физическом сервере, так и на виртуальной машине. Убедитесь, что выбранное устройство соответствует аппаратным и программным требованиям (см. стр. 69).

**Расположение Сервера администрирования**

Устройства, управляемые Сервером администрирования, могут располагаться:

- в локальном сегменте сети;
- в интернете;
- в демилитаризованной зоне (DMZ).

При этом Сервер администрирования также может быть расположен в следующих сегментах: технологическом, корпоративном, сегментах демилитаризованной зоны (DMZ).

При использовании Kaspersky Security Center для управления защитой изолированного сегмента сети, рекомендуется разворачивать Сервер администрирования в сегменте демилитаризованной зоны (DMZ) (см. стр. 122). Это позволит организовать полноценное сегментирование сетей и минимизировать возможные обращения в защищаемый сегмент, сохранив при этом возможности по управлению устройствами и доставке обновлений.

**Ограничение установки Сервера администрирования на контроллер домена, терминальный сервер или пользовательское устройство**

Категорически не рекомендуется устанавливать Сервер администрирования на контроллер домена, терминальный сервер или пользовательское устройство.

Рекомендуется предусмотреть функциональное разделение ключевых устройств сети. Это позволит сохранить работоспособность разных систем при выходе устройства из строя или при его компрометации. В это же время такой подход позволит реализовать различные политики безопасности для каждого устройства.

Например, ограничения безопасности, применяемые к контроллеру доменаhttps://docs.microsoft.com/ru-RU/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack, могут значительно снизить производительность Сервера администрирования и привести к невозможности использования некоторых его функций. Если привилегированный доступ к контроллеру домена получит злоумышленник, он может изменить, повредить или уничтожить базу данных Active Directory Domain Services (AD DS). При этом также будут скомпрометированы все системы и учетные записи, управляемые Active Directory.

**Учетные записи для установки и запуска Сервера администрирования**

Рекомендуется запустить установку Сервера администрирования под учетной записью локального администратора, чтобы избежать использования учетных записей домена для доступа к базе данных Сервера администрирования. Набор необходимых учетных записей и их прав (см. стр. 218) зависит от выбранного типа СУБД, местоположения СУБД и способа создания базы данных Сервера администрирования.

При установке Kaspersky Security Center автоматически формируются группы пользователей KLAdmins и KLOperators. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы KLAdmins и KLOperators создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются на устройстве с Сервером администрирования и в домене, в который входит устройство с Сервером администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на устройстве с Сервером администрирования.

Чтобы избежать создания групп KLAdmins и KLOperators в домене и, как следствие, **присвоения прав для управления Сервером администрирования вне устройства, на котором он установлен**, рекомендуется проводить установку Kaspersky Security Center под локальной учетной записью.

При установке Сервера администрирования выберите учетную запись, под которой Сервер администрирования будет запускаться как служба. По умолчанию приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования (klserver).

Служба Сервера администрирования при необходимости может запускаться под выбранной учетной записью. При этом учетная запись должна обладать различными правами для подключения к СУБД. Для обеспечения безопасности используйте непривилегированную учетную запись для запуска службы Сервера администрирования.

Во избежание некорректных параметров доступа для учетной записи Сервера администрирования рекомендуется создавать ее автоматически (см. стр. 249).

#### Исключение Сервера администрирования из домена

Не рекомендуется включать в домен устройство с Сервером администрирования (если оно используется). Это позволит разграничить права управления Kaspersky Security Center и избежать получения доступа к управлению в случае компрометации домена.

## Безопасность соединения

#### Использование TLS

Рекомендуется запретить небезопасные подключения к Серверу администрирования. Например, при настройке Сервера администрирования, рекомендуется не включать подключения по HTTP-протоколу к Серверу администрирования.

Обратите внимание, что по умолчанию часть HTTP-портов Сервера администрирования (см. стр. 98) закрыта. Оставшийся порт используется Веб-сервером Kaspersky Security Center (8060). Этот порт можно ограничить параметрами сетевого экрана устройства с Сервером администрирования.

#### Строгие параметры TLS

Рекомендуется использовать протокол TLS версии 1.2 или выше и ограничить или запретить использование небезопасных алгоритмов шифрования.

Вы можете настроить протоколы шифрования (см. стр. 313) (TLS), используемые Сервером администрирования. При этом учитывайте, что на момент выпуска определенной версии Сервера администрирования параметры протокола шифрования по умолчанию настроены так, чтобы обеспечить безопасную передачу данных.

#### Ограничение доступа к базе данных Сервера администрирования

Рекомендуется ограничить доступ к базе данных Сервера администрирования. Например, вы можете разрешить доступ только с устройства с Сервером администрирования. Это позволит снизить вероятность взлома базы Сервера администрирования данных через известные уязвимости.

Вы можете настроить параметры в соответствии с руководством по эксплуатации используемой базы данных, а также предусмотреть закрытые порты на сетевых экранах.

#### Запрет удаленной аутентификации с учетными записями Windows

Запрет на SSPI-подключения с удаленных адресов возможен с помощью специального флага LP_RestrictRemoteOsAuth. Этот флаг позволяет запретить удаленную аутентификацию на Сервере администрирования для учетных записей Windows, локальных или доменных.

*Чтобы переключить флаг LP_RestrictRemoteOsAuth в режим запрета SSPI-подключений с удаленных адресов:*

1. С помощью утилиты klscflag укажите значение флага LP_RestrictRemoteOsAuth:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

2. Перезапустите службу Сервера администрирования.

Флаг LP_RestrictRemoteOsAuth не работает, если удаленная аутентификация выполняется через Kaspersky Security Center 14.2 Web Console или Консоль администрирования, установленную на том же устройстве, что и Сервер администрирования.

#### Аутентификация Microsoft SQL Server

Если вы используете Microsoft SQL Server в качестве СУБД Сервера администрирования (см. стр. 247), нужно защитить от несанкционированного доступа данные Kaspersky Security Center, передаваемые в базу данных или получаемые от нее, а также данные, хранящиеся в этой базе данных. Для этого требуется настроить использование безопасного соединения между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь - это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обеих программ. Во всех других случаях рекомендуется использовать сертификат SSL/TLS для аутентификации экземпляра SQL Server (см. стр. 234).

#### Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором установлена Kaspersky Security Center 14.2 Web Console или Консоль администрирования на основе Microsoft Management Console (MMC). Настроить Сервер администрирования (см. стр. 678) можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, если злоумышленник похитит учетную запись Kaspersky Security Center, он сможет подключиться к Kaspersky Security Center только с тех IP-адресов, которые добавлены в разрешенные.

### Учетные записи и авторизация

#### Использование двухэтапной проверки Сервера администрирования

Kaspersky Security Center предоставляет пользователям Kaspersky Security Center Web Console и Консоли администрирования возможность использовать **двухэтапную проверку** (см. стр. 997) на основе стандарта RFC 6238 (TOTP: Time-Based One-Time Password algorithm).

Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center 14.2 Web Console или в Консоль администрирования вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию (на стр. 979) для своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение проверки подлинности на своем компьютере или мобильном устройстве.

Существуют как программные, так и аппаратные аутентификаторы (токены), поддерживающие стандарт RFC 6238. Например, к программным аутентификаторам относятся Google Authenticator, Microsoft Authenticator, FreeOTP.

Категорически не рекомендуется устанавливать приложение проверки подлинности на том же устройстве, с которого выполняется подключение к Серверу администрирования. Например, вы можете установить приложение для проверки подлинности на мобильном устройстве.

### Использование двухфакторной аутентификации операционной системы

Для авторизации на устройстве с Сервером администрирования рекомендуется использовать многофакторную аутентификацию (MFA) с использованием токена, смарт-карты или другого способа.

### Запрет на сохранение пароля администратора

При использовании Консоли администрирования не рекомендуется сохранять пароль администратора в диалоговом окне подключения к Серверу администрирования.

Также при работе с Сервером администрирования через Kaspersky Security Center 14.2 Web Console не рекомендуется сохранять пароль администратора в браузере на устройстве пользователя.

### Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Сервера администрирования (см. стр. 767) должен соответствовать следующим требованиям:

- Длина пароля должна быть от 8 до 16 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A-Z);
  - нижний регистр (A-Z) (a-z);
  - числа (0-9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля (см. стр. 768).

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

### Отдельная группа администрирования для устройства с Сервером администрирования

Для Сервера администрирования рекомендуется создать выделенную группу администрирования (см. стр. 709). Предоставьте этой группе особые права доступа (см. стр. 1216) и создайте политику безопасности для нее.

Чтобы избежать умышленного понижения уровня защиты Сервера администрирования рекомендуется ограничить список учетных записей, которые могут управлять этой группой администрирования.

### Группы KLAdmins и KLOperators

Группы пользователей KLAdmins и KLOperators (см. стр. 675) создаются автоматически во время установки Kaspersky Security Center. Группе KLAdmins предоставлены все права. Группе KLOperators предоставлены права на Чтение и Выполнение. Набор прав, предоставленных группе KLAdmins, **недоступен для изменения**.

С помощью стандартных средств администрирования операционной системы можно просмотреть группы KLAdmins и KLOperators и внести изменения в состав этих групп.

При разработке регламентов работы с Сервером администрирования нужно определить, потребуется ли специалисту информационной безопасности полный доступ (и включение в группу KLAdmins) для решения штатных задач.

Большинство базовых задач администрирования могут быть распределены между подразделениями организации (или разными сотрудниками одного подразделения) и, как следствие, между различными учетными записями. Также может быть выполнено разграничение по доступу к группам администрирования в Kaspersky Security Center. В результате можно реализовать такую модель использования, при которой авторизация под учетными записями из группы KLAdmins будет нестандартным поведением, что можно рассматривать как инцидент.

Если установка Kaspersky Security Center проводилась под системной учетной записью, группы создаются только на устройстве с Сервером администрирования. В этом случае рекомендуем убедиться, что в группу включены только учетные записи, созданные во время установки Kaspersky Security Center. Не рекомендуется добавлять в группу KLAdmins другие группы пользователей (локальные и/или доменные), которые были созданы автоматически во время установки Kaspersky Security Center. Группа KLAdmins должна включать единичные непривилегированные учетные записи.

Если установка выполнялась под учетной записью пользователя, входящего в домен, группы KLAdmins и KLOperators создаются как на Сервере администрирования, так и в домене, в который входит Сервер администрирования. Рекомендуется применить аналогичный подход как и в случае с установкой под системной учетной записью.

**Ограничить членство в роли "Главный администратор"**

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

По умолчанию после установки Сервера администрирования роль "Главный администратор" присвоена группе локальных администраторов устройства и созданной группе KLAdmins. Это удобно для управления, но критично с точки зрения безопасности, так как роль "Главный администратор" имеет очень широкий набор привилегий – назначение этой роли пользователям должно быть строго регламентировано.

Локальных администраторов можно исключить из списка пользователей, имеющих права администратора Kaspersky Security Center. Роль "Главный администратор" нельзя удалить из группы KLAdmins. В нее можно включить учетные записи группы KLAdmins (см. стр. 675), которые будут использоваться для управления Сервером администрирования.

В случае использования доменной аутентификации, рекомендуется ограничить привилегии учетных записей администраторов домена в Kaspersky Security Center. По умолчанию этим учетным записям присвоена роль "Главный администратор". Также администратор домена может включить свою учетную запись в группу KLAdmins с целью получения роли "Главный администратор". Чтобы этого избежать, в параметрах безопасности Kaspersky Security Center можно добавить группу "Администраторы домена" ("Domain Admins") и определить для нее запрещающие правила. Эти правила будут приоритетнее разрешающих.

Также можно использовать предопределенные роли пользователей (см. стр. 771) с уже настроенным набором прав.

**Запрет аутентификации с учетными записями Windows**

При компрометации устройства с Сервером администрирования в группу KLAdmins могут быть включены недоверенные учетные записи, что может привести к получению доступа к Серверу администрирования и возможностям администратора.

Вы можете запретить аутентификацию с использованием учетных записей Windows. Для этого добавьте встроенную группу "Все" (Everyone) и группу "Доменные пользователи" (Domain Users) в параметры безопасности и установите запрет на все параметры по управлению и получению доступа (при необходимости можно оставить права на чтение).

В группу "Все" (Everyone) входят все пользователи, даже анонимные пользователи и гости. Принадлежность к группе контролируется операционной системой.

Если вы запретите аутентификацию с учетными записями Windows, аутентификация на Сервере администрирования будет возможна только для внутренних пользователей. Перед включением этого параметра нужно убедиться, что создан как минимум один внутренний пользователь и ему присвоена роль "Главный администратор". Если текущий пользователь потеряет доступ к Серверу администрирования после применения этого параметра, Сервер администрирования отправит соответствующее уведомление.

Запрет на выполнение действий имеет больший приоритет, чем разрешающие правила, поэтому даже при включении пользователя в группу KLAdmins доступ к Серверу администрирования предоставлен не будет.

Перед включение параметра обязательно убедитесь, что созданы учетные записи внутренних администраторов. Некорректное использование этого параметра может привести к потере контроля над Сервером администрирования.

**Настройка прав доступа к функциям программы**

Рекомендуется использовать возможности гибкой настройки прав доступа (см. стр. 771) пользователей и групп пользователей к разным функциям Kaspersky Security Center.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты устройства и удаленной установкой стороннего программного обеспечения:

- Управление группами администрирования.
- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений (см. стр. 1450).

  Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с Сервером администрирования при возникновении события.

**Отдельная учетная запись для удаленной установки приложений**

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей (кроме "Главного администратора" или иной специализированной учетной записи).

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль (см. стр. 797) или разрешения (см. стр. 798) отдельной учетной записи.

### Обеспечение безопасности привилегированного доступа Windows

Рекомендуется рассмотреть рекомендации Microsoft по обеспечению безопасности привилегированного доступа. Чтобы просмотреть эти рекомендации, перейдите в раздел Обеспечение безопасности привилегированного доступа ( https://learn.microsoft.com/ru-RU/security/compass/overview). Одной из ключевых рекомендаций является развертывание рабочих станций с привилегированным доступом (PAW) https://learn.microsoft.com/ru-RU/security/compass/privileged-access-devices#paw-phased-implementation.

### Использование управляемых учетных записей служб (MSA) и групповых управляемых учетных записей служб (gMSA) для запуска служб Сервера администрирования

В Active Directory существует специальный тип учетных записей для безопасного запуска служб – MSA/gMSA https://learn.microsoft.com/ru-RU/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview. Kaspersky Security Center поддерживает управляемые учетные записи службы (см. стр. 249) (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

### Регулярный аудит всех пользователей

Рекомендуется проводить регулярный аудит всех пользователей на устройстве, где установлен Сервер администрирования. Это позволит реагировать на некоторые типы угроз безопасности, связанные с возможной компрометацией устройства.

## Управление защитой Сервера администрирования

### Выбор программы безопасности Сервера администрирования

Выбор приложения для защиты устройства, на котором установлен Сервер администрирования, зависит от типа развертывания Сервера администрирования и общей стратегии защиты.

Если вы разворачиваете Сервер администрирования на выделенном устройстве, рекомендуется выбрать программу Kaspersky Endpoint Security для защиты устройства с Сервером администрирования. Это позволит применить все имеющиеся технологии для защиты устройства, в том числе модули поведенческого анализа.

Если Сервер администрирования устанавливается на уже существующее в инфраструктуре устройство, использованное ранее для выполнения других задач, рекомендуются следующие приложения защиты:

- Kaspersky Industrial CyberSecurity for Nodes. Эту программу рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это программа, имеющая сертификаты совместимости с различными производителями промышленного программного обеспечения.
- Рекомендованные программы безопасности. Если Сервер администрирования установлен на устройство с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных программ (возможно, уже существуют рекомендации по выбору программы безопасности, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

### Создание отдельной политики безопасности для защиты программы

Для приложения защиты Сервера администрирования нужно создать отдельную политику безопасности. Эта политика должна отличаться от политики безопасности для клиентских устройств. Такой подход позволит задать максимально подходящие параметры безопасности для Сервера администрирования, не влияя при этом на уровень защиты других устройств.

Рекомендуется разделить устройства на группы, определив устройство с Сервером администрирования в отдельную группу администрирования, для которой вы затем можете создать специальную политику безопасности.

**Модули защиты**

Если отсутствуют особые рекомендации от производителя стороннего программного обеспечения, установленного на том же устройстве, что и Сервер администрирования, рекомендуется активировать и настроить все доступные модули защиты (после проверки их работы в течение определенного времени).

**Настройка сетевого экрана устройства с Сервером администрирования**

На устройстве с Сервером администрирования рекомендуется настроить сетевой экран таким образом, чтобы ограничить число устройств, с которых администраторы могут подключаться к Серверу администрирования через Консоль администрирования либо Kaspersky Security Center 14.2 Web Console.

По умолчанию Сервер администрирования использует порт (см. стр. 98) 13291 для подключения к Консоли администрирования и порт 13299 для подключения к Kaspersky Security Center 14.2 Web Console. Рекомендуется ограничить число устройств, с которых Сервер администрирования может управляться по этим портам.

**Запрет на запуск панели управления**

Если вы установили Сервер администрирования на устройство под управлением Microsoft Windows и используете приложение с модулем контроля запуска программ, можно запретить запуск панели управления (control.exe) для непривилегированных пользователей, например для группы администраторов.

В таком случае, после создания указанных запрещающих правил контроля запуска программ, пользователи с правами предустановленной роли Администратора потеряют возможность контролировать другие учетные записи сети, в том числе изменять имена учетных записей и пароли.

## Управление защитой клиентских устройств

**Ограничение добавления лицензионных ключей в инсталляционные пакеты**

Инсталляционные пакеты хранятся в папке общего доступа Сервера администрирования, во вложенной папке Packages. Если лицензионные ключи будут добавлены в инсталляционный пакет, они могут быть доступны на чтение всем пользователям, имеющим права на чтение этой папки общего доступа.

Для того чтобы избежать компрометации лицензионного ключа, не рекомендуется добавлять лицензионные ключи в инсталляционные пакеты.

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства (см. стр. 390), выполнять развертывание с помощью задачи Добавление лицензионного ключа для управляемой программы, и добавлять код активации или файл ключа на устройства вручную.

**Правила автоматического перемещения устройств между группами администрирования**

Рекомендуется ограничить использование правил автоматического перемещения устройств (см. стр. 336) между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования (см. стр. 157).

**Требования к безопасности к устройствам с точками распространения и шлюзам соединений**

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства в группе.
- Выполнять удаленную установку программ сторонних производителей и программ "Лаборатории Касперского" на клиентские устройства.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации используется для следующего:

- уменьшение нагрузки на Сервер администрирования;
- оптимизация трафика;
- предоставление Серверу администрирования доступа к устройствам в труднодоступных частях сети.

С учетом доступных возможностей рекомендуется защитить, в том числе физически, устройства, выполняющие роль точек распространения, от любого типа несанкционированного доступа.

**Ограничение автоматического назначения точек распространения**

Для упрощения администрирования и сохранения работоспособности сети рекомендуется воспользоваться автоматическим назначением точек распространения. Однако в промышленных и небольших сетях рекомендуется избегать автоматического назначения точек распространения, так как на точки распространения могут быть, например, переданы конфиденциальные сведения учетных записей, используемых для работы задач принудительной удаленной установки средствами операционной системы.

В промышленных и небольших сетях вы можете назначить точки распространения вручную (см. стр. 1266).

При необходимости вы также можете просмотреть Отчет о работе точек распространения (см. стр. 771).

## Настройка защиты управляемых приложений

**Политики управляемых приложений**

Рекомендуется создать политику (см. стр. 83) для каждого вида используемого приложения и компонента Kaspersky Security Center (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Agent и другие). Политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

**Установка пароля на выключение защиты и удаление приложения**

**Чтобы злоумышленники не могли отключить программы безопасности "Лаборатории Касперского", рекомендуется установить пароль для выключения защиты и удаления программ безопасности "Лаборатории Касперского".** Вы можете установить пароль, например, для Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/123303.htm, Kaspersky Security для Windows Servers, Агента администрирования (см. стр. 1083) и других программ "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

### Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Сервера администрирования рекомендуется использовать Kaspersky Security Network (KSN) (см. стр. 829) и принять актуальное Положение о KSN. При обновлении Сервера администрирования вы также можете принять обновленное Положение о KSN. Когда использование облачных служб запрещено законодательством или иными нормативными актами, вы можете не включать KSN.

### Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу (см. стр. 409), периодически запускающую полную проверку устройств.

### Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств (см. стр. 325): настроить интеграцию с Active Directory и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и политики по умолчанию, применяемые к этой группе.

### Определение папки общего доступа

Если Сервер администрирования развернут на устройстве под управлением Windows, при выборе существующей папки общего доступа (см. стр. 250), (которая используется, например, для размещения инсталляционных пакетов и хранилища обновляемых баз) рекомендуем убедиться, что права на чтение предоставлены группе "Все" (Everyone), а права на запись – группе KLAdmins.

## Обслуживание Сервера администрирования

### Резервное копирование данных Сервера администрирования

Резервное копирование данных позволяет восстановить данные Сервера администрирования без их потери (см. стр. 693). По умолчанию задача резервного копирования создается автоматически после установки Kaspersky Security Center и выполняется периодически с сохранением резервных копий в соответствующей директории.

Пользователь может изменить параметры задачи резервного копирования:

- увеличить частоту резервного копирования;
- определить особую директорию для сохранения копий;
- изменить пароль для резервной копии.

При хранении резервных копий в директории, отличной от директории по умолчанию, рекомендуется ограничить ACL этой директории. Учетные записи Сервера администрирования и сервера базы данных Сервера администрирования должны иметь доступ на запись в этой директории.

### Обслуживание Сервера администрирования

Обслуживание Сервера администрирования (см. стр. 870) позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (при необходимости).

**Обновление операционной системы и стороннего программного обеспечения на устройстве с Сервером администрирования**

Настоятельно рекомендуется регулярно выполнять установку обновлений операционной системы и стороннего программного обеспечения (см. стр. 488) на устройстве с Сервером администрирования.

Клиентским устройствам не требуется постоянное подключение к Серверу администрирования, поэтому после установки обновлений можно безопасно перезагрузить устройство с Сервером администрирования. Все события, зарегистрированные на клиентских устройствах во время простоя Сервера администрирования, отправляются на него после восстановления соединения.

### Передача событий в сторонние системы

**Мониторинг и отчеты**

Для своевременного реагирования на инциденты безопасности вы можете настроить функции мониторинга и параметры отчетов (см. стр. 1360).

**Экспорт событий в SIEM-системы**

Для максимально быстрого выявления инцидентов до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему (см. стр. 836).

**Уведомление по электронной почте о событиях аудита**

Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Kaspersky Security Center Cloud Console уведомлений (см. стр. 316) о публикуемых им событиях аудита (см. стр. 642), критических событиях (см. стр. 619), событиях отказа функционирования (см. стр. 625) и предупреждениях (см. стр. 631).

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.

## Подготовка к развертыванию

В этом разделе описаны шаги, которые вы должны выполнить перед развертыванием Kaspersky Security Center.

### В этом разделе



### Планирование развертывания Kaspersky Security Center

Этот раздел содержит информацию об оптимальных вариантах развертывания компонентов Kaspersky Security Center в сети организации в зависимости от следующих критериев:

- общего количества устройств;
- наличия организационно или географически обособленных подразделений (офисов, филиалов);
- наличия обособленных сетей, связанных узкими каналами;
- необходимости доступа к Серверу администрирования из интернета.

## См. также:

Основной сценарий установки....92

## В этом разделе



## Типовые способы развертывания системы защиты

В этом разделе описаны типовые способы развертывания системы защиты в сети организации с помощью Kaspersky Security Center.

Необходимо обеспечить защиту системы от несанкционированного доступа всех видов. Перед установкой программы на устройство рекомендуется установить все доступные обновления безопасности для операционной системы и обеспечить физическую защиту Серверов администрирования и точек распространения.

Вы можете развернуть систему защиты в сети организации с помощью Kaspersky Security Center, используя следующие схемы развертывания:

- Развертывание системы защиты средствами Kaspersky Security Center одним из следующих способов:
  - через Консоль администрирования;
  - через Kaspersky Security Center 14.2 Web Console.

  Установка программ "Лаборатории Касперского" на клиентские устройства и подключение клиентских устройств к Серверу администрирования происходит автоматически с помощью Kaspersky Security Center.

Основной схемой развертывания является развертывание системы защиты через Консоль администрирования. Использование Kaspersky Security Center 14.2 Web Console позволяет запускать установку программ "Лаборатории Касперского" через браузер.

- Развертывание системы защиты вручную с помощью автономных инсталляционных пакетов, сформированных в Kaspersky Security Center.

  Установка программ "Лаборатории Касперского" на клиентские устройства и рабочее место администратора производится вручную, параметры подключения клиентских устройств к Серверу администрирования задаются при установке Агента администрирования.

  Этот вариант развертывания рекомендуется применять в случаях, когда невозможно провести удаленную установку.

Kaspersky Security Center также позволяет разворачивать систему защиты с помощью групповых политик Active Directory®.

## О планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 100,000 устройств. Если общее количество устройств в сети организации превышает 100 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

3. Если в составе организации есть крупные географически удаленные офисы (филиалы) с собственными администраторами, целесообразно разместить в этих офисах Серверы администрирования. В противном случае такие офисы следует рассматривать как обособленные сети, связанные узкими каналами, см. стр. 167). В этом случае все устройства обособленной сети будут получать обновления с таких "локальных центров обновлений". Точки распространения могут загружать обновления как с Сервера администрирования (поведение по умолчанию), так и с размещенных в интернете серверов "Лаборатории Касперского" (см. стр. 171). На основании проведенного анализа ответить на следующие вопросы:

   - Возможно ли обслуживание всех клиентов одним Сервером администрирования или требуется иерархия Серверов администрирования?
   - Какая аппаратная конфигурация Серверов администрирования требуется для обслуживания всех клиентов за время, определенное в пункте 2?
   - Требуется ли использование точек распространения для снижения нагрузки на каналы связи?

После ответа на перечисленные вопросы вы можете составить набор допустимых структур защиты организации.

В сети организации можно использовать одну из следующих типовых структур защиты:

- Один Сервер администрирования. Все клиентские устройства подключены к одному Серверу администрирования. Роль точки распространения выполняет Сервер администрирования.
- Один Сервер администрирования с точками распространения. Все клиентские устройства подключены к одному Серверу администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.
- Иерархия Серверов администрирования. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. Роль точки распространения выполняет главный Сервер администрирования.

- Иерархия Серверов администрирования с точками распространения. Для каждого сегмента сети выделен отдельный Сервер администрирования, включенный в общую иерархию Серверов администрирования. В сети выделены клиентские устройства, выполняющие роль точек распространения.

### См. также:


Типовая конфигурация точек распространения:один офис.....659

Типовая конфигурация:несколько крупных офисов с собственными администраторами .....163

Типовая конфигурация:множество небольших изолированных офисов.....163

Основной сценарий установки.....92


## Типовые конфигурации Kaspersky Security Center

В этом разделе описаны следующие типовые конфигурации размещения компонентов Kaspersky Security Center в сети организации:

- один офис;
- несколько крупных географически распределенных офисов с собственными администраторами;
- множество небольших географически распределенных офисов.

### См. также:


Основной сценарий установки.....92


### В этом разделе


Типовая конфигурация:один офис.....162

Типовая конфигурация:несколько крупных офисов с собственными администраторами .....163

Типовая конфигурация:множество небольших изолированных офисов.....163


#### *Типовая конфигурация: один офис*

В сети организации может быть размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 100 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

Серверы администрирования могут быть размещены как во внутренней сети, так и в демилитаризованной зоне, в зависимости от того, нужен ли доступ к Серверам администрирования из интернета.

Если Серверов несколько, рекомендуется объединить их в иерархию. Наличие иерархии Серверов администрирования позволяет избежать дублирования политик и задач, работать со всем множеством управляемых устройств, как если бы они все управлялись одним Сервером администрирования (то есть выполнять поиск устройств, создавать выборки устройств, создавать отчеты).

## См. также:



### *Типовая конфигурация: несколько крупных офисов с собственными администраторами*

При наличии нескольких крупных удаленных офисов следует рассмотреть возможность размещения Серверов администрирования в каждом из офисов. По одному или по несколько Серверов администрирования в каждом офисе, в зависимости от количества клиентских устройств и доступного аппаратного обеспечения. В таком случае каждый из офисов может быть рассмотрен как "Типовая конфигурация: один офис (см. стр. 162)". Для упрощения администрирования все Серверы администрирования следует объединить в иерархию, возможно, многоуровневую.

При наличии сотрудников, которые перемещаются между офисами вместе с устройствами (ноутбуками), в политике Агента администрирования следует создать профили подключения Агента администрирования. Профили подключения Агента администрирования поддерживают только устройства с операционными системами Windows и macOS.

## См. также:



### *Типовая конфигурация: Множество небольших изолированных офисов*

Эта типовая конфигурация предусматривает один главный офис и множество небольших удаленных офисов, которые могут связываться с главным офисом через интернет. Каждый из удаленных офисов находится за Network Address Translation (далее также NAT), то есть подключение из одного удаленного офиса в другой невозможно, офисы изолированы друг от друга.

В главном офисе следует поместить Сервер администрирования, а в остальных офисах назначить по одной или по несколько точек распространения. Так как связь между офисами осуществляется через интернет, целесообразно создать для точек распространения задачу *Загрузка обновлений в хранилища точек распространения* (см. стр. 1244), так, чтобы точки распространения загружали обновления не с Сервера администрирования, а непосредственно с серверов "Лаборатории Касперского", локальной или сетевой папок.

Если в удаленном офисе часть устройств не имеет прямого доступа к Серверу администрирования (например, доступ к Серверу администрирования осуществляется через интернет, но доступ в интернет есть не у всех устройств), то точки распространения следует переключить в режим шлюза. В таком случае Агенты администрирования на устройствах в удаленном офисе будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть в удаленном офисе, целесообразно возложить выполнение этой функции на одну из точек распространения.

Сервер администрирования не сможет посылать уведомления на порт 15000 UDP управляемым устройствам, размещенным за NAT в удаленном офисе. Для решения этой проблемы целесообразно включить в свойствах устройств, являющихся точками распространения, режим постоянного соединения с Сервером администрирования (флажок **Не разрывать соединение с Сервером администрирования**).

Этот режим доступен, если общее количество точек распространения не превышает 300. Используйте push-серверы, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Дополнительную информацию см. в следующих разделах: Использование точки распространения в качестве извещающего сервера(см. стр. 668).

### См. также:


О точках распространения.....167

Порты, используемые Kaspersky Security Center.....98


## Установка системы управления базами данных

Установите систему управления базами данных (СУБД), которая будет использоваться Kaspersky Security Center. Для этой цели выберите поддерживаемую СУБД (см. стр. 69). Вы можете выбрать, например, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL или MariaDB.

Сведения о том, как установить выбранную СУБД, см. в документации к ней.

Если вы решили установить СУБД PostgreSQL или Postgres Pro, убедитесь, что вы указали пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

Если вы установите MariaDB (см. стр. 166), MySQL, PostgreSQL или Postgres Pro используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

### См. также:


Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center .....166


## Выбор СУБД

При выборе СУБД, используемой Сервером администрирования, следует руководствоваться количеством устройств, которые обслуживает Сервер администрирования.

В таблице ниже перечислены допустимые варианты СУБД и рекомендации и ограничения их использования.

*Таблица 24. Рекомендации и ограничения СУБД*

| СУБД | Рекомендации и ограничения |
|---|---|
| SQL Server Express Edition 2012 и выше | Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 10 000 устройств и не собираетесь использовать компонент Контроль программ (см. стр. 1338) для управляемых устройств.<br>Недопустимо совместное использование СУБД Server Express Edition Сервером администрирования и какой-либо другой программой.<br>База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**. |
| Локальный SQL Server Edition, отличный от Express, 2012 и выше | Нет ограничений. |
| Удаленный SQL Server Edition, отличный от Express, 2012 и выше | Допустимо только в случае, если оба устройства находятся в одном домене Windows®; если домены разные, то между ними должно быть установлено двустороннее отношение доверия. |
| Локальный или удаленный MySQL 5.5, 5.6 или 5.7 (версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 и 5.5.5 не поддерживаются) | Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 10 000 устройств и не собираетесь использовать компонент Контроль программ для управляемых устройств. |
| Локальный или удаленный MySQL 8.0.20 или выше | Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 50 000 устройств и не собираетесь использовать компонент Контроль программ для управляемых устройств. |
| Локальная или удаленная версия MariaDB (см. поддерживаемые версии (см. стр. 69)) | Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 20 000 устройств и не собираетесь использовать компонент Контроль программ для управляемых устройств. |
| PostgreSQL, Postgres Pro (см. поддерживаемые версии (см. стр. 69)) | Используйте эту СУБД, если вы планируете использовать один Сервер администрирования, менее чем для 50 000 устройств, и не собираетесь использовать компонент Контроль программ для управляемых устройств. |

Если в качестве СУБД вы используете SQL Server 2019 и у вас нет накопительного исправления CU12 или выше, после установки Kaspersky Security Center необходимо выполнить следующие действия:

1. Подключитесь к SQL-серверу с помощью SQL Management Studio.
2. Выполните следующую команду (если вы выбрали другое имя для базы данных (см. стр. 247), используйте это имя вместо KAV):

```
USE KAV
GO
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. Перезапустите службу SQL Server 2019.

В противном случае использование SQL Server 2019 может завершиться с ошибкой, например, "Во 'внутреннем' пуле ресурсов недостаточно памяти для выполнения запроса".

### См. также:

Учетные записи для работы с СУБД.....218

Основной сценарий установки.....92

## Настройка сервера MariaDB x64 для работы с Kaspersky Security Center

Kaspersky Security Center поддерживает СУБД MariaDB. Дополнительные сведения о поддерживаемых версиях MariaDB см. в 167.

### См. также:

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.....132

*Доступ в интернет: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне*

Сервер администрирования может располагаться во внутренней сети организации, а в демилитаризованной зоне сети может находиться устройство с Агентом администрирования, работающим в качестве шлюза соединения (см. стр 90) с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить (см. стр. 205) Агент администрирования. При установке Агента администрирования в окне мастера установки **Шлюз соединений** выбрать вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.
- Устройство с установленным шлюзом соединения необходимо добавить в качестве точки распространения (см. стр. 664). Когда вы добавляете шлюз соединения, в окне **Добавление точки распространения** выберите параметр **Выбрать** → **Добавить шлюз соединений**.
- Чтобы использовать интернет для подключения внешних настольных компьютеров к Серверу администрирования, необходимо изменить инсталляционный пакет Агента администрирования. В свойствах созданного инсталляционного пакета (см. стр. 306) выберите **Дополнительно** → **Подключаться к Серверу администрирования через шлюз соединений** свойствах созданного инсталляционного пакета.

Для шлюза соединений, находящегося в демилитаризованной зоне, Сервер администрирования создает сертификат, подписанный сертификатом Сервера администрирования. Если администратор принял решение задать Серверу администрирования пользовательский сертификат, то это следует сделать до создания шлюза соединений в демилитаризованной зоне.

При наличии сотрудников с ноутбуками, которые могут подключаться к Серверу администрирования как из локальной сети, так и из интернета, может быть целесообразно создать в политике Агента администрирования правило переключения Агента администрирования.

kaspersky

## О точках распространения

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Раздавать обновления, причем обновления могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае для устройства, являющегося точкой распространения, должна быть создана задача *Загрузка обновлений в хранилища точек распространения* (см. стр. 465):
  - Устанавливать программное обеспечение на другие устройства, в том числе выполнять первоначальное развертывание Агентов администрирования на устройствах.
  - Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшение нагрузки на Сервер администрирования.
- Оптимизация трафика.
- Предоставление Серверу администрирования доступ к устройствам в труднодоступных частях сети организации. Наличие точки распространения в находящейся за NAT (по отношению к Серверу администрирования) сети позволяет Серверу администрирования выполнять следующие действия:
  - отправлять уведомления на устройства через UDP в IPv4-сети или IPv6-сети;
  - опрос IPv4-сети или IPv6-сети;
  - выполнять первоначальное развертывание;
  - использовать в качестве push-сервера (см. стр. 668).

Точка распространения назначается на группу администрирования. В этом случае областью действия точки распространения будут устройства, находящиеся в этой группе администрирования и всех ее подгруппах. При этом устройство, являющееся точкой распространения, не обязано находиться в группе администрирования, на которую она назначена.

Вы можете сделать точку распространения шлюзом соединений. В этом случае, устройства, находящиеся в области действия точки распространения, будут подключаться к Серверу администрирования не напрямую, а через шлюз. Данный режим полезен в сценариях, когда между Сервером администрирования и управляемыми устройствами невозможно прямое соединение.

## См. также:


Настройка точек распространения и шлюзов соединений .....658

Основной сценарий установки.....92


## Расчет количества и конфигурации точек распространения

Чем больше клиентских устройств содержит сеть, тем больше требуется точек распространения. Рекомендуется не отключать автоматическое назначение точек распространения. При включенном автоматическом назначении точек распространения Сервер администрирования назначает точки распространения, если число клиентских устройств достаточно велико, и определяет их конфигурацию.

**Использование специально выделенных точек распространения**

Если вы планируете использовать в качестве точек распространения какие-то определенные устройства (например, выделенные для этого серверы), то можно не использовать автоматическое назначение точек распространения. В этом случае убедитесь, что устройства, которые вы хотите назначить точками распространения, имеют достаточно свободного места на диске, их не отключают регулярно и на них выключен "спящий режим".

*Таблица 25. Число уникально назначенных точек распространения в сети, содержащей один сегмент, в зависимости от количества сетевых устройств*

| Число клиентских устройств в каждом из сегментов сети | Количество точек распространения |
|---|---|
| Менее 300 | 0 (точки распространения не нужны) |
| Более 300 | Приемлемо: (N/10000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети |

*Таблица 26. Число уникально назначенных точек распространения в сети, содержащей несколько сегментов, в зависимости от количества сетевых устройств*

| Число клиентских устройств в сегменте сети | Количество точек распространения |
|---|---|
| Менее 10 | 0 (точки распространения не нужны) |
| 10 – 100 | 1 |
| Более 100 | Приемлемо: (N/10000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети |

**Использование клиентских устройств (рабочих станций) в качестве точек распространения**

Если вы планируете использовать в качестве точек распространения обычное клиентское устройство (рабочую станцию), то рекомендуется назначать точку распространения, как показано в таблице ниже, чтобы избежать чрезмерной нагрузки на каналы связи и Сервер администрирования:

*Таблица 27. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит один сегмент сети, в зависимости от количества сетевых устройств*

| Число клиентских устройств в каждом из сегментов сети | Количество точек распространения |
|---|---|
| Менее 300 | 0 (точки распространения не нужны) |
| Более 300 | (N/300 +1), где N – число устройств в сети; не менее 3 точек распространения |

*Таблица 28. Число рабочих станций, выполняющих роль точек распространения в сети, которая содержит несколько сегментов сети, в зависимости от количества сетевых устройств*

| Число клиентских устройств в сегменте сети | Количество точек распространения |
|---|---|
| Менее 10 | 0 (точки распространения не нужны) |
| 10 – 30 | 1 |
| 31 – 300 | 2 |
| Более 300 | (N/300 +1), где N – число устройств в сети; не менее 3 точек распространения |

Если точка распространения отключена или по другим причинам недоступна, то управляемые устройства из области действия этой точки распространения могут обращаться за обновлениями к Серверу администрирования.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Типовая конфигурация:множество небольших изолированных офисов.....163

## Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

## Виртуальные Серверы администрирования;

В рамках физического Сервера администрирования можно создать несколько виртуальных Серверов администрирования, во многом подобных подчиненным Серверам. По сравнению с моделью разделения доступа, основанной на списках контроля доступа (ACL), модель виртуальных Серверов более функциональна и предоставляет большую степень изоляции. Помимо собственной структуры групп администрирования для распределенных устройств с политиками и задачами, каждый виртуальный Сервер администрирования имеет также собственную группу нераспределенных устройств, собственные наборы отчетов, выборок устройств и событий, инсталляционных пакетов, правил перемещения устройств и так далее. Функциональность виртуальных Серверов администрирования может быть использована как поставщиками услуг для максимальной изоляции разных заказчиков друг от друга, так и крупными организациями со сложной структурой и большим количеством администраторов.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;

- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра программ и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

## Информация об ограничениях Kaspersky Security Center

В таблице ниже приведены ограничения текущей версии Kaspersky Security Center.

*Таблица 29. Ограничения Kaspersky Security Center*

| Тип ограничения | Значение |
|---|---|
| Максимальное количество управляемых устройств на один Сервер администрирования | 100 000 |
| Максимальное количество устройств с выбранным параметром **Не разрывать соединение с Сервером администрирования** | 300 |
| Максимальное количество групп администрирования | 10 000 |
| Максимальное количество хранимых событий | 45 000 000 |
| Максимальное количество политик | 2000 |
| Максимальное количество задач | 2000 |
| Максимальное суммарное количество объектов Active Directory (подразделений и учетных записей пользователей, устройств и групп безопасности) | 1 000 000 |
| Максимальное количество профилей в политике | 100 |
| Максимальное количество подчиненных Серверов у одного главного Сервера администрирования | 500 |
| Максимальное количество виртуальных Серверов администрирования | 500 |
| Максимальное количество устройств, которые может обслуживать одна точка распространения (точки распространения могут обслуживать только немобильные устройства) | 10 000 |
| Максимальное количество устройств, которые могут использовать один шлюз соединения | 10 000, включая мобильные устройства |
| Максимальное количество мобильных устройств на один Сервер администрирования | 100 000 минус количество стационарных управляемых устройств |

## Нагрузка на сеть

В этом разделе приводится информация об объеме сетевого трафика, которым обмениваются между собой клиентские устройства и Сервер администрирования в ходе выполнения ключевых административных сценариев.

Основная нагрузка на сеть связана с выполнением следующих административных сценариев:

- Первоначальное развертывание антивирусной защиты.
- Первоначальное обновление антивирусных баз.
- Синхронизация клиентского устройства с Сервером администрирования.
- Регулярное обновление антивирусных баз.
- Обработка событий на клиентских устройствах Сервером администрирования.

## В этом разделе



### *Первоначальное развертывание антивирусной защиты*

В этом разделе приведен расход трафика при установке на клиентском устройстве Агента администрирования версии и Kaspersky Endpoint Security для Windows (см. таблицу ниже).

Агент администрирования устанавливается путем принудительной установки, когда требуемые для установки файлы копируются Сервером администрирования в папку общего доступа на клиентском устройстве. После установки Агент администрирования получает дистрибутив Kaspersky Endpoint Security для Windows, используя соединение с Сервером администрирования.

*Таблица 30. Расход трафика*

| Сценарий | Установка Агента администрирования для одного клиентского устройства | Установка Kaspersky Endpoint Security для Windows для одного клиентского устройства (с обновленными базами) | Совместная установка Агента администрирования и Kaspersky Endpoint Security для Windows |
|---|---|---|---|
| Трафик от клиентского устройства к Серверу администрирования, КБ | 1638,4 | 7843,84 | 9707,52 |
| Трафик от Сервера администрирования к клиентскому устройству, КБ | 69990,4 | 259317,76 | 329318,4 |
| Общий трафик (для одного клиентского устройства), КБ | 71628,8 | 267161,6 | 339025,92 |

После установки Агентов администрирования на клиентские устройства можно назначить одно из устройств в группе администрирования точкой распространения. Он будет использоваться для распространения инсталляционных пакетов. В этом случае объем трафика, передаваемого при первоначальном развертывании антивирусной защиты, существенно отличается в зависимости от того, используется ли многоадресная IP-рассылка.

В случае использования многоадресной IP-рассылки инсталляционные пакеты рассылаются один раз по всем включенным устройствам в группе администрирования. Таким образом, общий трафик уменьшится примерно в N раз, где N – общее число включенных устройств в группе администрирования. Если многоадресная IP-рассылка не используется, общий трафик совпадает с трафиком загрузки инсталляционных пакетов с Сервера администрирования. При этом источником инсталляционных пакетов является точка распространения, а не Сервер администрирования.

### *Первоначальное обновление антивирусных баз*

Скорости трафика при первичном обновлении антивирусных баз (при первом запуске задачи обновления баз на клиентском устройстве) следующие:

- Трафик от клиентского устройства к Серверу администрирования: 1,8 МБ.
- Трафик от Сервера администрирования к клиентскому устройству: 113 МБ.
- Общий трафик (для одного клиентского устройства): 114 МБ.

Данные могут несколько отличаться в зависимости от текущей версии антивирусных баз.

### *Синхронизация клиента с Сервером администрирования*

Этот сценарий характеризует состояние системы администрирования в случае, когда происходит активная синхронизация данных между клиентским устройством и Сервером администрирования. Клиентские устройства подключаются к Серверу администрирования с периодом, заданным администратором. Сервер администрирования сравнивает состояние данных на клиентском устройстве с состоянием данных на Сервере, регистрирует данные о последнем подключении клиентского устройства в базе данных и проводит синхронизацию данных.

В разделе приведена информация о расходе трафика для основных административных сценариев при подключении клиента к Серверу администрирования с синхронизацией (см. таблицу ниже). Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

*Таблица 31. Расход трафика*

| Сценарий | Трафик от клиентских устройств к Серверу администрирования, КБ | Трафик от Сервера администрирования к клиентским устройствам, КБ | Общий трафик (для одного клиентского устройства), КБ |
|---|---|---|---|
| Первоначальная синхронизация до обновления баз на клиентском устройстве | 699,44 | 568,42 | 1267,86 |
| Первоначальная синхронизация после обновления баз на клиентском устройстве | 735,8 | 4474,88 | 5210,68 |
| Синхронизация при отсутствии изменений на клиентском устройстве и на Сервере администрирования | 11,99 | 6,73 | 18,72 |
| Синхронизация при изменении одного параметра в политике группы | 9,79 | 11,39 | 21,18 |
| Синхронизация при изменении одного параметра в групповой задаче | 11,27 | 11,72 | 22,99 |
| Принудительная синхронизация при отсутствии изменений на клиентском устройстве | 77,59 | 99,45 | 177,04 |

Объем общего трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

Объем трафика при первоначальной синхронизации до и после обновления баз указан для следующих случаев:

- установка на клиентское устройство Агента администрирования и программы безопасности;
- перенос клиентского устройства в группу администрирования;
- применение к клиентскому устройству политики и задач, созданных для группы по умолчанию.

В таблице указан объем трафика при изменении одного из параметров защиты, входящих в параметры политики Kaspersky Endpoint Security. Данные для других параметров политики могут отличаться от данных, представленных в таблице.

### *Добавочное обновление антивирусных баз*

Расход трафика при инкрементальном обновлении антивирусных баз спустя 20 часов после предыдущего обновления следующий:

- Трафик от клиентского устройства к Серверу администрирования: 169 кБ.
- Трафик от Сервера администрирования к клиентскому устройству: 16 МБ.
- Общий трафик (для одного клиентского устройства): 16,3 МБ.

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусных баз.

Объем трафика существенно изменяется в зависимости от того, используется ли многоадресная IP-рассылка внутри групп администрирования. В случае использования многоадресной IP-рассылки общий трафик для группы уменьшается примерно в N раз, где N – число включенных устройств в группе администрирования.

### *Обработка событий клиентов Сервером администрирования*

В этом разделе приведен расход трафика при возникновении на клиентском устройстве события "Найден вирус", информация о котором передается на Сервер администрирования и регистрируется в базе данных (см. таблицу ниже).

*Таблица 32. Расход трафика*

| Сценарий | Передача на Сервер администрирования данных при наступлении события "Найден вирус" | Передача на Сервер администрирования данных при наступлении девяти событий "Найден вирус" |
|---|---|---|
| Трафик от клиентского устройства к Серверу администрирования, КБ | 49,66 | 64,05 |
| Трафик от Сервера администрирования к клиентскому устройству, КБ | 28,64 | 31,97 |
| Общий трафик (для одного клиентского устройства), КБ | 78,3 | 96,02 |

Данные, приведенные в таблице, могут несколько отличаться в зависимости от текущей версии антивирусной программы и в зависимости от того, какие именно события определены в политике как требующие регистрации в базе данных Сервера администрирования.

*Расход трафика за сутки*

В этом разделе приведена информация о расходе трафика за сутки работы системы администрирования в состоянии "покоя", когда не происходит изменений данных ни со стороны клиентских устройств, ни со стороны Сервера администрирования (см. таблицу ниже).

Данные, приведенные в таблице, характеризуют состояние сети после стандартной установки Kaspersky Security Center и завершения работы мастера первоначальной настройки. Период синхронизации клиентского устройства с Сервером администрирования составлял 20 минут, загрузка обновлений в хранилище Сервера администрирования происходила каждый час.

*Таблица 33. Уровень трафика за сутки в состоянии простоя*

| Поток трафика | Значение |
|---|---|
| Трафик от клиентского устройства к Серверу администрирования, КБ | 3235,84 |
| Трафик от Сервера администрирования к клиентскому устройству, КБ | 64378,88 |
| Общий трафик (для одного клиентского устройства), КБ | 67614,72 |

## Сведения о производительности Сервера администрирования

В разделе представлены результаты тестирования производительности Сервера администрирования для разных аппаратных конфигураций, а также ограничения на подключение управляемых устройств к Серверу администрирования.

### В этом разделе



### Ограничения подключений к Серверу администрирования

Сервер администрирования поддерживает управление до 100 000 устройств без потери производительности.

Ограничения на подключения к Серверу администрирования без потери производительности:

- Один Сервер администрирования может поддерживать до 500 виртуальных Серверов администрирования.
- Главный Сервер администрирования поддерживает одновременно не более 1000 сессий.
- Виртуальные Серверы администрирования поддерживают одновременно не более 1000 сессий.

### См. также:

## Результаты тестов производительности Сервера администрирования

Результаты тестов производительности Сервера администрирования позволили определить максимальные количества клиентских устройств, с которыми Сервер администрирования может выполнить синхронизацию за указанные промежутки времени. Вы можете использовать эту информацию для выбора оптимальной схемы развертывания антивирусной защиты в компьютерных сетях.

Для тестирования использовались устройства со следующими аппаратными конфигурациями (см. таблицы ниже):

*Таблица 34. Аппаратная конфигурация Сервера администрирования*

| Параметр | Значение |
|---|---|
| Процессор | Intel Xeon CPU E5630, тактовая частота 2,53 ГГц, 2 сокет, 8 ядер, 16 логических процессоров |
| ОЗУ | 26 ГБ |
| Жесткий диск | IBM ServeRAID M5014 SCSI Disk Device, 487 ГБ |
| Операционная система | Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763 |
| Сеть | QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client) |

*Таблица 35. Аппаратная конфигурация устройства с SQL Server*

| Параметр | Значение |
|---|---|
| Процессор | Intel Xeon CPU X5570, тактовая частота 2,93 ГГц, 2 сокет, 8 ядер, 16 логических процессоров |
| ОЗУ | 32 ГБ |
| Жесткий диск | Adaptec Array SCSI Disk Device, 2047 ГБ |
| Операционная система | Microsoft Windows Server 2019 Standard, версия 10.0.17763, сборка 17763 |
| Сеть | Intel 82576 Gigabit |

Сервер администрирования поддерживал создание 500 виртуальных Серверов администрирования.

Период синхронизации составлял по 15 минут на каждые 10 000 управляемых устройств (см. таблицу ниже).

*Таблица 36. Обобщенные результаты нагрузочного тестирования Сервера администрирования*

| Период синхронизации, мин. | Количество управляемых устройств |
|---|---|
| 15 | 10 000 |
| 30 | 20 000 |
| 45 | 30 000 |
| 60 | 40 000 |
| 75 | 50 000 |
| 90 | 60 000 |
| 105 | 70 000 |
| 120 | 80 000 |
| 135 | 90 000 |
| 150 | 100 000 |

При подключении Сервера администрирования к серверу базы данных MySQL и SQL Express не рекомендуется использовать программу для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

## Результаты тестирования производительности прокси-сервера KSN

Если ваша корпоративная сеть включает в себя большое количество клиентских устройств, и они используют Сервер администрирования в качестве прокси-сервера KSN, Сервер администрирования должен удовлетворять определенным аппаратным требованиям, чтобы обрабатывать запросы с клиентских устройств. Вы можете использовать результаты тестирования ниже для оценки загрузки Сервера администрирования в вашей сети и планирования аппаратных ресурсов, для обеспечения нормальной работы службы прокси-сервера KSN.

В таблице ниже приведена конфигурация аппаратного обеспечения Сервера администрирования и SQL Server. Эта конфигурация была использована для тестирования.

*Таблица 37. Аппаратная конфигурация Сервера администрирования*

| Параметр | Значение |
|---|---|
| Процессор | Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров |
| ОЗУ | 32 ГБ |
| Операционная система | Microsoft Windows Server 2016 Standard |

*Таблица 38. Аппаратная конфигурация SQL Server*

| Параметр | Значение |
|---|---|
| Процессор | Intel Xeon CPU E5450, тактовая частота 3,00 ГГц, 2 сокет, 8 ядер, 16 логических процессоров |
| ОЗУ | 32 ГБ |
| Операционная система | Microsoft Windows Server 2019 Standard |

В таблице ниже приведены результаты тестирования.

*Таблица 39. Обобщенные результаты тестирования производительности прокси-сервера KSN*

| Параметр | Значение |
|---|---|
| Максимальное количество обработанных запросов в секунду | 4914 |
| Максимальное использование процессора | 36% |

# Развертывание Агента администрирования и программы безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загрузка обновлений напрямую с серверов "Лаборатории Касперского" (если выполняет роль точки распространения); функционирование в качестве прокси-сервера KSN (если выполняет роль точки распространения); и обнаружение уязвимостей программ сторонних производителей (при использовании Системного администрирования).

## В этом разделе

## Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная инсталляция программ на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемой программы вместе с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентами администрирования и Сервером администрирования. Для передачи дистрибутива можно использовать промежуточные центры распространения в виде точек распространения, многоадресную рассылку и прочие средства. Подробные сведения об установке программ на управляемые устройства, на которых уже установлен Агент администрирования, см. далее в этом разделе.

Первоначальную установку Агента администрирования на устройства на платформе Microsoft Windows можно осуществлять следующими способами:

- С помощью сторонних средств удаленной установки программ.
- Путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования: средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков, или сторонними средствами.
- Через механизм групповых политик Microsoft Windows: с помощью штатных средств управления групповыми политиками Microsoft Windows или автоматизированно, с помощью соответствующего параметра в задаче удаленной установки программ Kaspersky Security Center.
- Принудительно с помощью соответствующих параметров в задаче удаленной установки программ Kaspersky Security Center.
- Путем рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center. Автономные пакеты представляют собой исполняемые модули, содержащие в себе дистрибутивы выбранных программ с настроенными параметрами.
- Вручную, запуская инсталляторы программ на устройствах.

На платформах, отличных от Microsoft Windows, первоначальную установку Агента администрирования на управляемых устройствах следует осуществлять имеющимися сторонними средствами. Обновлять Агент администрирования до новой версии, а также устанавливать другие программы "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки программ, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания программ в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурация сети организации (см. стр. 162);
- общего количества устройств;
- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности использование UAC и режима Simple File Sharing).

kaspersky

## В этом разделе



## Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети программ "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки программы. При установке Агента администрирования требуется задать по крайней мере адрес для подключения к Серверу администрирования, а возможно, и некоторые дополнительные параметры. В зависимости от выбранного способа установки параметры можно задавать различными способами. В простейшем случае (при интерактивной установке вручную на выбранное устройство) необходимые параметры можно задать с помощью пользовательского интерфейса инсталлятора.

Этот способ настройки параметров не подходит для неинтерактивной "тихой" установки программ на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для неинтерактивной установки на выбранные устройства в сети.

## Инсталляционные пакеты;

Первый и основной способ настройки инсталляционных параметров приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в собственном формате (.msi, .deb, .rpm) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров инсталляции, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. стр. 236).

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

- Инструкцию по использованию этого способа настройки программ "Лаборатории Касперского" перед развертыванием с помощью сторонних инструментов см. на стр. 192).

## Развертывание при помощи сторонних средств удаленной установки приложений

При наличии в организации каких-либо средств удаленной установки приложений (например, Microsoft System Center) целесообразно выполнять первоначальное развертывание при помощи этих средств.

Нужно выполнить следующие действия:

- Выбрать способ настройки параметров инсталляции, наиболее подходящий для используемого средства развертывания.
- Определить механизм синхронизации между изменением параметров инсталляционных пакетов через интерфейс Консоли администрирования и работой выбранных сторонних средств развертывания приложений из данных инсталляционных пакетов.
- В случае установки из папки общего доступа убедиться в достаточной производительности этого файлового ресурса.

## См. также:



## О задачах удаленной установки программ Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска, установка с помощью групповых политик Microsoft Windows). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Консоли администрирования в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и / или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

## Развертывание захватом и копированием образа устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа устройства.

► *Чтобы выполнить развертывание путем захвата и копирования жесткого диска:*

1. Создать эталонное устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и программу безопасности.
2. Захватить образ "эталонного" устройства и далее распространять этот образ на новые устройства посредством задачи Kaspersky Security Center.

   Для захвата и установки образов диска можно воспользоваться как имеющимися в организации сторонними средствами, так и функциональностью, предоставляемой (при наличии лицензии на Системное администрирование) Kaspersky Security Center (см. стр. 805).

Если для работы с образами диска используются сторонние инструменты, необходимо при развертывании на устройство из эталонного образа обеспечить удаление информации, с помощью которой Kaspersky Security Center идентифицирует управляемое устройство. В противном случае Сервер администрирования не сможет в дальнейшем корректно различать устройства, созданные путем копирования одного и того же образа (см. стр. 868).
При захвате образа диска средствами Kaspersky Security Center эта проблема решается автоматически.

**Копирование образа жесткого диска сторонними инструментами**

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- Рекомендуемый метод. При установке Агента администрирования на эталонное устройство (см. стр. 868) захватить образ устройства до первого запуска службы Агента администрирования (так как

уникальная информация, идентифицирующая устройство, создается при первом подключении Агента администрирования к Серверу администрирования). В дальнейшем рекомендуется не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.

- На эталонном устройстве остановить службу Агента администрирования и запустить утилиту klmover с ключом -dupfix. Утилита klmover входит в состав инсталляционного пакета Агента администрирования. В дальнейшем не допускать запуск службы Агента администрирования вплоть до выполнения операции захвата образа.
- Обеспечить запуск утилиты klmover с ключом -dupfix до (это важно) первого запуска службы Агента администрирования на устройствах при первом старте операционной системы после развертывания образа. Утилита klmover входит в состав инсталляционного пакета Агента администрирования.
- Используйте режим клонирования диска Агента администрирования. (см. стр. 867).

Если образ жесткого диска был скопирован неправильно, вы можете решить эту проблему (см. стр. 183).

Также можно захватить образ устройства без установленного Агента администрирования. Для этого выполните развертывание образа на целевых устройствах, а затем установите Агент администрирования. При использовании этого метода предоставьте доступ к сетевой папке с автономными инсталляционными пакетами с устройства (см. стр. 805).

## См. также:



## Неверно выполнено копирование образа жесткого диска

Если копирование образа жесткого диска с установленным Агентом администрирования было выполнено без учета правил развертывания (см. стр. 182), часть устройств в Консоли администрирования может отображаться как один значок устройства, постоянно меняющий имя.

Можно использовать следующие способы решения этой проблемы:

- Удаление Агента администрирования.

  Этот способ является самым надежным. На устройствах, которые были скопированы из образа неправильно, нужно при помощи сторонних средств удалить Агент администрирования, а затем установить его заново. Удаление Агента администрирования не может быть выполнено средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

- Запуск утилиты klmover с ключом "-dupfix".

  На проблемных устройствах (на всех, которые были скопированы из образа неправильно) необходимо при помощи сторонних средств однократно запустить утилиту klmover с ключом "-dupfix" (klmover -dupfix), расположенную в папке установки Агента администрирования. Запуск утилиты не может быть выполнен средствами Kaspersky Security Center, поскольку для Сервера администрирования все проблемные устройства неразличимы (им всем соответствует один и тот же значок в Консоли администрирования).

  Затем следует удалить значок, на который отображались проблемные устройства до запуска утилиты.

- Ужесточение правила обнаружения неправильно скопированных устройств.

Этот способ можно использовать только в случае, если установлены Сервер администрирования и Агенты администрирования версии 10 Service Pack 1 или новее.

Следует ужесточить правило обнаружения неправильно скопированных Агентов администрирования таким образом, чтобы изменение NetBIOS-имени устройства приводило к автоматической "починке" таких Агентов администрирования (предполагается, что скопированные устройства имеют различные NetBIOS-имена).

На устройстве с Сервером администрирования нужно импортировать в Реестр представленный ниже reg-файл и перезапустить службу Сервера администрирования.

- Если на устройстве с Сервером администрирования установлена 32-разрядная операционная система:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

- Если на устройстве с Сервером администрирования установлена 64-разрядная операционная система:

```
REGEDIT4
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
"KLSRV_CheckClones"=dword:00000003
```

## Развертывание с помощью механизма групповых политик Microsoft Windows

Первоначальное развертывание Агентов администрирования рекомендуется осуществлять с помощью групповых политик Microsoft Windows при выполнении следующих условий:

- устройства являются членами домена Active Directory;
- план развертывания позволяет дождаться штатной перезагрузки устройств до начала развертывания на них Агентов администрирования, или к устройствам можно принудительно применить групповую политику Windows.

Суть данного способа развертывания заключается в следующем:

- Дистрибутив приложения в формате Microsoft Installer (MSI-пакет) размещается в папке общего доступа (в папке, к которой имеют доступ на чтение учетные записи LocalSystem устройств).
- В групповой политике Active Directory создается объект установки данного дистрибутива.
- Область действия установки задается привязкой к организационному подразделению и / или к группе безопасности, в которую входят устройства.
- При очередном входе устройства в домен (до входа в систему пользователей устройства) выполняется проверка наличия требуемого приложения среди установленных приложений. Если приложение отсутствует, происходит загрузка дистрибутива с заданного в политике ресурса и его установка.

Одним из преимуществ этого способа развертывания является то, что назначенные приложения устанавливаются на устройства при загрузке операционной системы еще до входа пользователя в систему.

Даже если пользователь, имеющий необходимые права, удалит приложение, при следующей загрузке операционной системы оно будет установлено снова. Недостатком этого способа развертывания является то, что произведенные администратором изменения в групповой политике не вступят в силу до перезагрузки устройств (без применения дополнительных средств).

С помощью групповых политик можно устанавливать как Агент администрирования, так и другие приложения, инсталляторы которых имеют формат Windows Installer.

При выборе этого способа развертывания, помимо прочего, необходимо оценить нагрузку на файловый ресурс, с которого будет осуществляться копирование файлов на устройства при применении групповой политики Windows.

**Работа с политиками Microsoft Windows с помощью задачи удаленной установки приложений Kaspersky Security Center**

Самым простым способом инсталляции приложений при помощи групповых политик Microsoft Windows является включение параметра **Назначить установку инсталляционного пакета в групповых политиках Active Directory** в свойствах задачи удаленной установки приложений Kaspersky Security Center. В этом случае при запуске задачи Сервер администрирования самостоятельно выполнит следующие действия:

- Создаст необходимые объекты в групповой политике Microsoft Windows.
- Создаст специальные группы безопасности, в которые включит устройства, и назначит установку выбранных приложений для этих групп безопасности. Состав групп безопасности будет актуализироваться при каждом запуске задачи в соответствии с набором устройств на момент запуска.

Для обеспечения работоспособности данной функции следует указать в параметрах задачи учетную запись, имеющую права на редактирование групповых политик Active Directory.

Если с помощью одной задачи предполагается установить и Агент администрирования, и другое приложение, включение флажка **Назначить установку инсталляционного пакета в групповых политиках Active Directory** приведет к созданию в политике Active Directory объекта установки только для Агента администрирования. Второе выбранное в задаче приложение будет устанавливаться уже средствами Агента администрирования, как только он будет установлен на устройстве. Если по какой-то причине необходимо установить отличное от Агента администрирования приложение именно с помощью групповых политик Windows, то нужно создать задачу установки только для этого инсталляционного пакета (без пакета Агента администрирования). Не все приложения могут быть установлены с помощью групповых политик Microsoft Windows. О такой возможности вы можете узнать, обратившись к информации о способах установки приложения.

В случае, когда необходимые объекты создаются в групповой политике средствами Kaspersky Security Center, в качестве источника инсталляционного пакета будет использована папка общего доступа Kaspersky Security Center. При планировании развертывания следует соотнести скорость чтения из этой папки с количеством устройств и размером устанавливаемого дистрибутива. Возможно, будет целесообразно расположить папку общего доступа Kaspersky Security Center в мощном специализированном файловом хранилище (см. стр. 236).

Помимо простоты, автоматическое создание групповых политик Windows средствами Kaspersky Security Center имеет еще одно преимущество: при планировании установки Агента администрирования легко указать группу администрирования Kaspersky Security Center, в которую будут автоматически перемещаться устройства по завершении установки. Группу можно указать в мастере создания задачи или в окне параметров задачи удаленной установки.

При работе с групповыми политиками Windows средствами Kaspersky Security Center задание устройств для объекта групповой политики осуществляется путем создания группы безопасности. Kaspersky Security Center синхронизирует состав группы безопасности с текущим набором устройств задачи. При использовании иных средств для работы с групповыми политиками можно привязывать объекты групповых политик непосредственно к выбранным подразделениям Active Directory.

**Самостоятельная установка приложений с помощью политик Microsoft Windows**

Администратор может самостоятельно создать в групповой политике Windows объекты, необходимые для установки. В этом случае можно сослаться на пакеты, лежащие в папке общего доступа Kaspersky Security Center, или выложить пакеты на отдельный файловый сервер и сослаться на них.

Возможны следующие сценарии установки:

- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Объект групповой политики ссылается на MSI-файл этого сконфигурированного пакета, лежащего в папке общего доступа Kaspersky Security Center.
- Администратор создает инсталляционный пакет и настраивает его свойства в Консоли администрирования. Затем администратор копирует целиком подпапку EXEC этого пакета из папки общего доступа Kaspersky Security Center в папку на специализированном файловом ресурсе организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации.
- Администратор загружает дистрибутив приложения (в том числе дистрибутив Агента администрирования) из интернета и выкладывает его на специализированный файловый ресурс организации. Объект групповой политики ссылается MSI-файл этого пакета, лежащего в подпапке на специализированном файловом ресурсе организации. Настройка параметров инсталляции осуществляется путем настройки свойств MSI или настройкой файлов трансформации MSI (см. стр. 192).

## См. также:

Установка программы с помощью групповых политик Active Directory.....363

## Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

В случае если требуется начать развертывание Агентов администрирования или других необходимых программ немедленно, без ожидания очередного входа устройств в домен, или же при наличии устройств, не являющихся членами домена Active Directory, можно использовать принудительную установку выбранных инсталляционных пакетов при помощи задачи удаленной установки Kaspersky Security Center.

Устройства при этом могут задаваться явно (списком) либо выбором группы администрирования Kaspersky Security Center, которой они принадлежат, либо созданием выборки устройств по определенному условию. Время запуска установки определяется расписанием задачи. Если в свойствах задачи включен параметр **Запускать пропущенные задачи**, задача может запускаться сразу при включении устройств или при переносе их в целевую группу администрирования.

Данный способ установки осуществляется путем копирования файлов на административный ресурс admin$ каждого из устройств и удаленной регистрации на них вспомогательных служб. При этом должны выполняться следующие условия:

- Устройства должны быть доступны для подключения либо со стороны Сервера администрирования, либо со стороны точки распространения.
- В сети должно корректно работать разрешение имен для устройств.
- На управляемых устройствах не должны быть отключены административные ресурсы общего доступа admin$.
- На устройствах должна быть запущена системная служба Server (по умолчанию данная служба запущена).
- Следующие порты должны быть открыты на целевых устройствах для обеспечения удаленного доступа с помощью инструментов Windows: TCP 139, TCP 445, UDP 137 и UDP 138.
- На устройствах должен быть выключен режим Simple File Sharing.
- На устройствах модель совместного доступа и безопасности для локальных учетных записей должна находиться в состоянии *Обычная – локальные пользователи удостоверяются как они сами* (Classic – local users authenticate as themselves), и ни в коем случае не в состоянии *Гостевая – локальные пользователи удостоверяются как гости* (Guest only – local users authenticate as Guest).
- Устройства должны быть членами домена, либо на устройствах должны быть заблаговременно созданы унифицированные учетные записи с административными правами.

Устройства, расположенные в рабочих группах, могут быть приведены в соответствие указанным выше требованиям при помощи утилиты riprep.exe, которая описана на портале Службы технической поддержки "Лаборатории Касперского".

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Можно использовать упрощенный способ создания задач принудительной установки приложений – автоматическую установку. Для этого в свойствах группы администрирования нужно выбрать в списке инсталляционных пакетов те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне. Для работоспособности принудительной установки необходимо обеспечить наличие точек распространения в каждой такой изолированной сети.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети. Однако следует учитывать, что данный

способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Поэтому нужно выбирать в качестве точек распространения мощные устройства с высокопроизводительными накопителями. Также необходимо, чтобы объем свободного места в разделе с папкой %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit многократно превосходил суммарный объем дистрибутивов устанавливаемых программ.

## Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный инсталляционный пакет размещается в папке общего доступа Kaspersky Security Center.

При помощи Kaspersky Security Center можно разослать по электронной почте выбранным пользователям ссылку на этот файл в папке общего доступа с просьбой запустить файл (интерактивно или с ключом "тихой" установки "-s"). Автономный инсталляционный пакет можно прикрепить к сообщению электронной почты для пользователей устройств, не имеющих доступа к папке общего доступа Kaspersky Security Center. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого приложения (например, программы безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в "тихом" режиме (при запуске с ключом "-s"). "Тихий" режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в "тихом" режиме определяется кодом возврата процесса.

## Возможности ручной установки приложений

Администраторы или опытные пользователи могут устанавливать приложения вручную в интерактивном режиме. При этом можно использовать как исходные дистрибутивы, так и сформированные из них инсталляционные пакеты, расположенные в папке общего доступа Kaspersky Security Center. Инсталляторы по умолчанию работают в интерактивном режиме, запрашивая у пользователя все необходимые значения параметров. Но при запуске процесса setup.exe из корня инсталляционного пакета с ключом "-s" инсталлятор будет работать в "тихом" режиме с параметрами, заданными при настройке инсталляционного пакета.

> При запуске setup.exe из корня инсталляционного пакета расположенного в папке общего доступа Kaspersky Security Center, сначала произойдет копирование пакета во временную локальную папку, затем из локальной папки будет запущен инсталлятор приложения.

## Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается параметром **С помощью Агента администрирования** в свойствах задачи удаленной установки приложений (см. стр. 181).

Если параметр выбран, то передача на устройства инсталляционных пакетов с заданными администратором инсталляционными параметрами осуществляется по каналам связи между Агентом администрирования и Сервером администрирования.

Для оптимизации нагрузки на Сервер администрирования и минимизации трафика между Сервером администрирования и устройствами целесообразно назначать в каждой удаленной сети или в каждом широковещательном домене точки распространения (см. стр. 658). В этом случае распространение инсталляционных пакетов и параметров инсталлятора осуществляется с Сервера администрирования на устройства через точки распространения.

Также с использованием точек распространения можно выполнять широковещательную (многоадресную) рассылку инсталляционных пакетов, что позволяет многократно снизить сетевой трафик в ходе развертывания программ.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. При использовании большого числа различных инсталляционных пакетов большого размера и при большом количестве точек распространения размер этой папки может существенно увеличиваться.

Удалять файлы из папки FTServer вручную нельзя. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTClTmp.

Удалять файлы из папки $FTClTmp вручную нельзя. По мере завершения задач, использующих данные из папки, содержимое этой папки будет удаляться автоматически.

Поскольку инсталляционные пакеты распространяются по каналам связи между Сервером администрирования и Агентами администрирования из промежуточного хранилища в оптимизированном для передачи по сети формате, нельзя вносить изменения в инсталляционные пакеты в исходной папке инсталляционного пакета. Такие изменения не будут автоматически учтены Сервером администрирования. Если необходимо изменить вручную файлы инсталляционных пакетов (хотя делать это не рекомендуется), нужно обязательно изменить какие-либо параметры инсталляционного пакета в Консоли администрирования. Изменение параметров инсталляционного пакета в Консоли администрирования заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

## Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки программ Kaspersky Security Center, в мастере создания задачи или в окне свойств созданной задачи (раздел **Перезагрузка операционной системы**) можно выбрать вариант действия при необходимости перезагрузки устройства с операционной системой Windows:

- **Не перезагружать устройство**. В этом случае автоматическая перезагрузка не будет выполнена. Для завершения установки потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки будет сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач установки на серверы и другие устройства, для которых критически важна бесперебойная работа.
- **Перезагрузить устройство**. В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения установки. Этот вариант подходит для задач установки на устройства, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
- **Запрашивать у пользователя**. На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Вариант **Запрашивать у пользователя** наиболее подходит для рабочих станций, пользователи которых должны иметь возможность выбрать наиболее подходящий момент для перезагрузки.

## Целесообразность обновления баз в инсталляционном пакете программы безопасности

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом программы безопасности. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах.

## Использование средств удаленной установки приложений Kaspersky Security Center для запуска на управляемых устройствах произвольных исполняемых файлов

С помощью мастера создания инсталляционного пакета можно выбрать произвольный исполняемый файл и задать для него параметры командной строки. При этом в инсталляционный пакет можно поместить как сам выбранный файл, так и всю папку, в которой этот файл содержится. Затем следует создать задачу удаленной установки и выбрать созданный инсталляционный пакет.

В ходе работы задачи на устройствах будет запущен указанный при создании исполняемый файл с заданными параметрами командной строки.

Если используются инсталляторы в формате Microsoft Windows Installer (MSI), Kaspersky Security Center использует штатные возможности по анализу результата установки.

Если есть лицензия на Системное администрирование, при создании инсталляционного пакета для одного из поддерживаемых приложений, распространенных в корпоративной среде, Kaspersky Security Center также использует правила установки и анализа результатов установки, имеющиеся в его обновляемой базе.

В иных случаях для исполняемых файлов задача по умолчанию дожидается завершения запущенного процесса и всех порожденных им дочерних процессов. По завершении запущенных процессов задача будет завершена успешно независимо от кода возврата исходного процесса. Чтобы изменить такое поведение задачи, перед созданием задачи следует изменить вручную файлы с расширением kpd, сформированные Kaspersky Security Center в папке созданного инсталляционного пакета и в его подпапках.

Для того чтобы задача не ожидала завершения запущенного процесса, в секции [SetupProcessResult] нужно задать значение 0 для параметра Wait:

**Пример:**

```
[SetupProcessResult]
Wait=0
```

Для того чтобы на платформе Windows задача ожидала только завершения исходного процесса, но не порожденных им дочерних процессов, нужно в секции [SetupProcessResult] задать значение 0 для параметра WaitJob, например:

**Пример:**

```
[SetupProcessResult]
WaitJob=0
```

Для того чтобы задача завершалась успешно или с ошибкой в зависимости от кода возврата запущенного процесса, нужно перечислить успешные коды возврата в секции [SetupProcessResult_SuccessCodes], например:

**Пример:**

```
[SetupProcessResult_SuccessCodes]
0=
3010=
```

В этом случае любой код, отличный от перечисленных, будет означать ошибку.

Для того чтобы в результатах задачи отображалась строка с комментарием об успешном завершении задачи или сообщения об ошибках, нужно задать краткие описания ошибок, соответствующих кодам возврата процесса, в секциях [SetupProcessResult_SuccessCodes] и [SetupProcessResult_ErrorCodes], например:

**Пример:**

```
[SetupProcessResult_SuccessCodes]
0 = установка завершена успешно
3010=A reboot is required to complete the installation
[SetupProcessResult_ErrorCodes]
1602=Installation cancelled by the user
1603 = критическая ошибка при установке
```

Для того чтобы задействовать средства Kaspersky Security Center по управлению перезагрузкой устройства (если перезагрузка необходима для завершения операции), нужно дополнительно перечислить коды возврата процесса, означающие необходимость перезагрузки, в секции [SetupProcessResult_NeedReboot]:

**Пример:**

[SetupProcessResult_NeedReboot]

3010=

## Мониторинг развертывания

Для контроля развертывания Kaspersky Security Center, а также для контроля наличия на управляемых устройствах программы безопасности и Агента администрирования, следует обращать внимание на цветовой индикатор в блоке **Развертывание**. Индикатор расположен в рабочей области узла Сервер администрирования в главном окне Консоли администрирования (см. стр. 578). Индикатор отображает текущее состояние развертывания. Рядом с индикатором отображается количество устройств с установленными Агентами администрирования и программами безопасности. При наличии активных задач установки отображается прогресс выполнения задач. При наличии ошибок установки, здесь отображается количество ошибок. Просмотреть детальную информацию об ошибке можно по ссылке.

Также можно воспользоваться диаграммой развертывания в рабочей области папки **Управляемые устройства** на закладке **Группы**. Диаграмма отражает процесс развертывания: количество устройств без Агента администрирования, с Агентом администрирования, с Агентом администрирования и программой безопасности.

Более детальное описание хода развертывания (или работы конкретной задачи установки) можно увидеть в окне результатов выполнения соответствующей задачи удаленной установки: В контекстном меню задачи выберите **Результаты**. В окне отображаются два списка: в верхнем списке содержится список состояний задачи на устройствах, а в нижнем – список событий задачи на устройстве, которое в данный момент выбрано в верхнем списке.

Информация об ошибках при развертывании записывается в журнал событий Kaspersky Event Log Сервера администрирования. Информация об ошибках также доступна в соответствующей выборке событий в узле Сервера администрирования на закладке **События**.

## Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в "тихом" режиме.

### В этом разделе

kaspersky

## Общая информация

Инсталляторы компонентов Kaspersky Security Center – Сервера администрирования, Агента администрирования, Консоли администрирования – построены на технологии Windows Installer. Ядром инсталлятора является MSI-пакет. Этот формат упаковки дистрибутива позволяет использовать все преимущества технологии Windows Installer: масштабируемость, возможность использовать систему патчевания, систему трансформации, возможность установки централизованно сторонними решениями, прозрачность регистрации в операционной системе.

## См. также:



## Установка в тихом режиме (с файлом ответов)

В инсталляторах Сервера администрирования и Агента администрирования реализована возможность работы с файлом ответов (ss_install.xml), в котором записаны параметры для установки в тихом режиме без участия пользователя. Файл ss_install.xml расположен в той же папке, что и MSI-пакет, и используется автоматически при установке в тихом режиме. Вы можете включить режим автоматической установки с помощью ключа командной строки "/s".

Пример запуска:

```
setup.exe /s
```

Прежде чем запускать программу установки в тихом режиме, прочтите Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.

Файл ss_install.xml представляет собой внутренний формат параметров инсталлятора Kaspersky Security Center. В составе дистрибутивов поставляется файл ss_install.xml с параметрами по умолчанию.

Не следует изменять файл ss_install.xml вручную. Этот файл изменяется средствами Kaspersky Security Center при изменении параметров инсталляционных пакетов в Консоли администрирования.

► *Чтобы изменить файл ответов для установки Сервера администрирования:*

1. Откройте дистрибутив Kaspersky Security Center. Если вы используете полный пакет EXE-файла, распакуйте его.
2. Сформируйте папку Сервер, откройте командную строку и выполните следующую команду:

```
setup.exe /r ss_install.xml
```

Запущен установщик Kaspersky Security Center installer.

3. Следуйте инструкциям мастера, чтобы настроить установку Kaspersky Security Center.

По завершении работы мастера файл ответов автоматически изменится в соответствии с новыми параметрами, указанными вами.

## См. также:



## Установка Агента администрирования в тихом режиме (без файла ответов)

Агент администрирования можно установить при помощи одного только msi-пакета, задавая при этом значения свойств MSI стандартным образом. Такой сценарий позволяет устанавливать Агент администрирования, используя групповые политики. Для того чтобы не возникал конфликт между параметрами, заданными с помощью свойств MSI, и параметрами, заданными в файле ответов, предусмотрена возможность отключения файла ответов путем задания свойства `DONT_USE_ANSWER_FILE=1`. Ниже приведен пример запуска инсталлятора Агента администрирования с помощью msi-пакета.

Установка Агента администрирования в неинтерактивном режиме требует принятия Лицензионного соглашения (см. стр. 343). Используйте параметр `EULA=1`, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

**Пример:**

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Также параметры инсталляции msi-пакета можно задать, подготовив предварительно файл трансформации (файл с расширением mst). Команда будет выглядеть следующим образом:

**Пример:**

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

В одной команде можно указать более одного файла трансформации.

## См. также:



## Частичная настройка параметров установки через setup.exe

Запуская установку программ через setup.exe, можно передавать в MSI-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

**Пример:**

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

## См. также:



## Параметры установки Сервера администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Сервера администрирования. Все параметры являются необязательными, кроме EULA и PRIVACYPOLICY.

*Таблица 40. Параметры установки Сервера администрирования в неинтерактивном режиме*

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| EULA | Согласие с условиями лицензии (обязательный параметр). | • 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. стр. 343).<br>• Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется). |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| PRIVACYPOLICY | Согласие с условиями Политики конфиденциальности (обязательный параметр). | • 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности (см. стр. 216). Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности.<br>• Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется). |
| INSTALLATIONMODETYPE | Тип установки Сервера администрирования. | • Обычный.<br>• Пользовательская. |
| INSTALLDIR | Папка установки программы. | Строковое значение. |
| ADDLOCAL | Список компонентов для установки (через запятую). | CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.<br>Минимальный достаточный для корректной установки Сервера администрирования список компонентов:<br>`ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86` |
| NETRANGETYPE | Размер сети. | • NRT_1_100 – от 100 до 100 устройств.<br>• NRT_100_1000 – от 101 до 1000 устройств.<br>• NRT_GREATER_1000 – более 1000 устройств. |
| SRV_ACCOUNT_TYPE | Способ задания пользователя для работы службы Сервера администрирования. | • SrvAccountDefault – учетная запись пользователя будет создана автоматически.<br>• SrvAccountUser – учетная запись пользователя задана вручную. |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| SERVERACCOUNTNAME | Имя пользователя для службы. | Строковое значение. |
| SERVERACCOUNTPWD | Пароль пользователя для службы. | Строковое значение. |
| DBTYPE | Тип базы данных. | • MySQL – будет использоваться база данных MySQL или MariaDB.<br>• MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Server Express). |
| MYSQLSERVERNAME | Полное имя базы данных сервера MySQL или MariaDB. | Строковое значение. |
| MYSQLSERVERPORT | Номер порта для подключения к базе данных сервера MySQL или MariaDB. | Числовое значение. |
| MYSQLDBNAME | Имя базы данных сервера MySQL или MariaDB. | Строковое значение. |
| MYSQLACCOUNTNAME | Имя пользователя для подключения к базе mysql-сервера. | Строковое значение. |
| MYSQLACCOUNTPWD | Пароль пользователя для подключения к базе данных сервера MySQL или MariaDB. | Строковое значение. |
| MSSQLCONNECTIONTYPE | Тип использования базы данных MSSQL. | • InstallMSSEE – установить из пакета.<br>• ChooseExisting – использовать установленный сервер. |
| MSSQLSERVERNAME | Полное имя экземпляра SQL Server. | Строковое значение. |
| MSSQLDBNAME | Имя базы данных SQL Server. | Строковое значение. |
| MSSQLAUTHTYPE | Способ аутентификации при подключении к SQL Server. | • Windows.<br>• SQLServer. |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| MSSQLACCOUNTNAME | Имя пользователя для подключения к SQL Server в режиме SQLServer. | Строковое значение. |
| MSSQLACCOUNTPWD | Пароль пользователя для подключения к SQL Server в режиме SQLServer. | Строковое значение. |
| CREATE_SHARE_TYPE | Способ задания папки общего доступа. | • Create – создать новую папку общего доступа; в этом случае должны быть заданы свойства:<br>  • SHARELOCALPATH – путь к локальной папке.<br>  • SHAREFOLDERNAME – сетевое имя папки.<br>• Пусто – должно быть задано свойство EXISTSHAREFOLDERNAME. |
| EXISTSHAREFOLDERNAME | Полный путь к существующей папке общего доступа. | Строковое значение. |
| SERVERPORT | Номер порта для подключения к Серверу администрирования. | Числовое значение. |
| SERVERSSLPORT | Номер порта для установки SSL-соединения с Сервером администрирования. | Числовое значение. |
| SERVERADDRESS | адрес Сервера администрирования; | Строковое значение. |
| SERVERCERT2048BITS | Длина ключа для сертификата Сервера администрирования (в битах). | • 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит.<br>• 0 – длина ключа для сертификата Сервера администрирования составляет 1024 бит.<br>• Если параметр не задан, длина ключа для сертификата Сервера администрирования составляет 1024 бит. |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| MOBILESERVERADDRESS | Адрес Сервера администрирования для подключения мобильных устройств; игнорируется, если не выбран компонент MobileSupport. | Строковое значение. |

## См. также:



## Параметры установки Агента администрирования

В таблице ниже описаны свойства MSI, которые можно настраивать при установке Агента администрирования. Все параметры являются необязательными, кроме EULA и SERVERADDRESS.

*Таблица 41. Параметры установки Агента администрирования в неинтерактивном режиме*

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| EULA | Согласие с условиями Лицензионного соглашения. | • 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. стр. 343).<br>• 0 – Я не принимаю условия Лицензионного соглашения (установка не выполняется).<br>• Значение не задано – Я не принимаю условия Лицензионного соглашения (установка не выполняется). |
| DONT_USE_ANSWER_FILE | Читать параметры установки из файла ответов. | • 1 – Не использовать.<br>• другое значение или не задано – читать. |
| INSTALLDIR | Путь к папке установки Агента администрирования. | Строковое значение. |
| SERVERADDRESS | Адрес Сервера администрирования (обязательный параметр). | Строковое значение. |
| SERVERPORT | Номер порта подключения к Серверу администрирования. | Числовое значение. |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| SERVERSSLPORT | Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL. | Числовое значение. |
| USESSL | Использовать ли SSL-соединение. | • 1 – использовать;<br>• другое значение или не задано – не использовать. |
| OPENUDPPORT | Открыть ли UDP-порт. | • 1 – открывать;<br>• другое значение или не задано – не открывать. |
| UDPPORT | Номер UDP-порта | Числовое значение. |
| USEPROXY | Использовать ли прокси-сервер. | • 1 – использовать;<br>• другое значение или не задано – не использовать. |
| PROXYLOCATION (PROXYADDRESS:PROXYPORT) | Адрес прокси-сервера и номер порта для подключения к прокси-серверу. | Строковое значение. |
| PROXYLOGIN | Учетная запись для подключения к прокси-серверу. | Строковое значение. |
| PROXYPASSWORD | Пароль учетной записи для подключения к прокси-серверу (указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей). | Строковое значение. |
| GATEWAYMODE | Режим использования шлюза соединения. | • 0 – не использовать шлюз соединений;<br>• 1 – использовать данный Агент администрирования в качестве шлюза соединений;<br>• 2 – подключаться к Серверу администрирования через шлюз соединений. |
| GATEWAYADDRESS | Адрес шлюза соединений. | Строковое значение. |

| Свойство MSI | Описание | Доступные значения |
|---|---|---|
| CERTSELECTION | Способ получения сертификата. | • GetOnFirstConnection – получить сертификат от Сервера администрирования;<br>• GetExistent – задать существующий сертификат. Если выбран этот вариант, должно быть задано свойство CERTFILE. |
| CERTFILE | Путь к файлу сертификата. | Строковое значение. |
| VMVDI | Включить динамический режим для VDI. | • 1 – включать;<br>• 0 – не включать;<br>• Значение не задано – не включать. |
| LAUNCHPROGRAM | Запускать ли службу Агента администрирования после установки. | • 1 – запускать;<br>• другое значение или не задано – не запускать. |
| NAGENTTAGS | Тег для Агента администрирования (имеет приоритет над тегом, указанным в файле ответов). | Строковое значение. |

## См. также:



## Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и программы безопасности на каждую виртуальную машину, а также вы можете защищать виртуальные машины на уровне гипервизора. В первом случае для защиты виртуальных машин можно использовать как обычную программу безопасности, так и Kaspersky Security для виртуальных сред Легкий агент. Во втором случае вы можете использовать Kaspersky Security для виртуальных сред Защита без агента.

Kaspersky Security Center поддерживает откат виртуальных машин к предыдущему состоянию (см. стр. 204).

## См. также:



## В этом разделе



## Рекомендации по снижению нагрузки на виртуальные машины

В случае инсталляции Агента администрирования на виртуальную машину следует рассмотреть возможность отключения той части функциональности Kaspersky Security Center, которая не очень полезна для виртуальных машин.

При установке Агента администрирования на виртуальную машину или на шаблон, из которого в дальнейшем будут получены виртуальные машины, рекомендуется выполнить следующие действия:

- Если выполняется удаленная установка, в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) включите параметр **Оптимизировать параметры для VDI**.
- если выполняется интерактивная установка с помощью мастера, в окне мастера выбрать параметр **Оптимизировать параметры Агента администрирования для виртуальной инфраструктуры**.

Выбор параметров изменит параметры Агента администрирования таким образом, чтобы по умолчанию (до применения политики) были выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

Как правило, перечисленные функции не нужны на виртуальных машинах в силу того, что программное обеспечение и виртуальное аппаратное обеспечение на них единообразны.

Выключение функций обратимо. Если любая из выключенных функций все же нужна, ее можно включить при помощи политики Агента администрирования, или в локальных параметрах Агента администрирования. Локальные параметры Агента администрирования доступны из контекстного меню соответствующего устройства в Консоли администрирования.

## См. также:



## Поддержка динамических виртуальных машин

Kaspersky Security Center поддерживает динамические виртуальные машины. Если в сети организации развернута виртуальная инфраструктура, то в некоторых случаях могут использоваться динамические (временные) виртуальные машины. Такие машины создаются с уникальными именами из заранее подготовленного администратором шаблона. Пользователь работает с созданной машиной некоторое время, а после выключения виртуальная машина удаляется из виртуальной инфраструктуры. Если в сети

организации развернут Kaspersky Security Center, то виртуальная машина с установленным на ней Агентом администрирования добавляется в базу данных Сервера администрирования. После выключения виртуальной машины запись о ней должна быть также удалена и из базы данных Сервера администрирования.

Чтобы функциональность автоматического удаления записей о виртуальных машинах работала, при установке Агента администрирования на шаблон, из которого будут созданы динамические виртуальные машины, нужно включить параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) (см. стр. 212);
- в случае интерактивной установки – в мастере установки Агента администрирования.

Параметр **Включить динамический режим для VDI** не следует включать при установке Агента администрирования на физические устройства.

Если нужно, чтобы события с динамических виртуальных машин сохранялись на Сервере администрирования некоторое время после удаления машин, то следует в окне свойств Сервера администрирования в разделе **Хранилище событий** включить параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

### См. также:

Основной сценарий установки.....92

## Поддержка копирования виртуальных машин

Копирование виртуальной машины с установленным на нее Агентом администрирования или ее создание из шаблона с установленным Агентом администрирования эквивалентно развертыванию Агентов администрирования захватом и копированием образа жесткого диска. Поэтому в общем случае при копировании виртуальных машин нужно выполнять те же действия, что и при развертывании копированием образа диска (см. стр. 182).

Однако в описанных ниже двух случаях Агент администрирования обнаруживает факт копирования автоматически. Поэтому выполнять сложные действия, описанные в разделе "Развертывание захватом и копированием жесткого диска устройства", необязательно:

- При установке Агента администрирования был включен параметр **Включить динамический режим для VDI**: после каждой перезагрузки операционной системы такая виртуальная машина будет считаться новым устройством, независимо от факта ее копирования.
- Используется один из следующих гипервизоров: VMware™, HyperV® или Xen®: Агент администрирования определит факт копирования виртуальной машины по изменившимся идентификаторам виртуального аппаратного обеспечения.

Анализ изменений виртуального аппаратного обеспечения не абсолютно надежен. Прежде чем широко использовать данный метод, следует предварительно проверить его работоспособность на небольшом количестве виртуальных машин для используемой в организации версии гипервизора.

См. также:

Основной сценарий установки.....92

## Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенной программой. Откат файловой системы в предыдущее состояние на одном из устройств с установленным Агентом администрирования приведет к рассинхронизации данных и неправильной работе Kaspersky Security Center.

Откат файловой системы (или ее части) в предыдущее состояние может происходить в следующих случаях:

- при копировании образа жесткого диска;
- при восстановлении состояния виртуальной машины средствами виртуальной инфраструктуры;
- при восстановлении данных из резервной копии или точки восстановления.

Для Kaspersky Security Center критичны только те сценарии, при которых стороннее программное обеспечение на устройствах с установленным Агентом администрирования затрагивает папку %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\. Поэтому следует всегда исключать эту папку из процедуры восстановления, если это возможно.

Поскольку в ряде организаций регламент работы предполагает выполнение отката состояния файловой системы устройств, в Kaspersky Security Center, начиная с версии 10 Maintenance Release 1 (Сервер администрирования и Агенты администрирования должны быть версии 10 Maintenance Release 1 или выше), была добавлена поддержка обнаружения отката файловой системы на устройствах с установленным Агентом администрирования. В случае обнаружения такие устройства автоматически переподключаются к Серверу администрирования с полной очисткой и полной синхронизацией данных.

В Kaspersky Security Center поддержка обнаружения отката файловой системы включена по умолчанию.

Следует при любой возможности избегать отката папки %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ на устройствах с установленным Агентом администрирования, так как полная повторная синхронизация данных требует большого количества ресурсов.

Для устройства с установленным Сервером администрирования откат состояния системы недопустим. Недопустимым также является откат в предыдущее состояние базы данных, используемой Сервером администрирования.

Восстановить состояние Сервера администрирования из резервной копии можно только при помощи штатной утилиты klbackup (см. стр. 689).

## Локальная установка программ

В этом разделе описана процедура установки программ, которые могут быть установлены на устройства только локально.

Для проведения локальной установки программ на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► *Чтобы установить программы локально на выбранное клиентское устройство:*

1. Установите на клиентское устройство Агент администрирования и настройте связь клиентского устройства с Сервером администрирования.
2. Установите на устройство необходимые программы согласно описаниям, изложенным в Руководствах к этим программам.
3. Установите на рабочее место администратора плагин управления для каждой из установленных программ.

Kaspersky Security Center также поддерживает возможность локальной установки программ с помощью автономного инсталляционного пакета. Kaspersky Security Center не поддерживает установку всех программ "Лаборатории Касперского" (см. стр. 69).

## См. также:



## В этом разделе



## Локальная установка Агента администрирования

► *Чтобы установить Агент администрирования на устройство локально:*

1. На устройстве запустите файл setup.exe из дистрибутива, полученного через интернет.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.
2. В окне с выбором программ по ссылке **Установить только Агент администрирования Kaspersky Security Center** запустите мастер установки Агента администрирования. Следуйте далее указаниям мастера.

   Во время работы мастера установки вы можете настроить дополнительные параметры Агента администрирования (см. ниже).
3. Чтобы использовать устройство в качестве шлюза соединений для выбранной группы администрирования, в окне **Шлюз соединений** мастера установки выберите вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**.

4. Чтобы настроить Агент администрирования при установке на виртуальную машину:

   a. Если вы планируете создать динамически виртуальные машины из образов виртуальных машин, включите динамический режим Агента администрирования для Virtual Desktop Infrastructure (VDI). Для этого в окне мастера установки **Дополнительные параметры** включите параметр **Включить динамический режим для VDI**.

      Пропустите этот шаг, если вы не планируете создавать динамически виртуальные машины из образов виртуальных машин.

   b. Оптимизируйте работу Агента администрирования для виртуальной инфраструктуры. Для этого в окне мастера установки **Дополнительные параметры** выберите параметр **Оптимизировать параметры Агента администрирования Kaspersky Security Center для виртуальной инфраструктуры**.

      В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

      - о реестре оборудования;
      - о программах, установленных на устройстве;
      - об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
      - об уязвимостях программного обеспечения, обнаруженных на локальном клиентском устройстве.

      В дальнейшем вы сможете включить передачу этой информации в свойствах Агента администрирования или в параметрах политики Агента администрирования.

   По окончании работы мастера установки Агент администрирования будет установлен на устройстве.

Вы можете просмотреть свойства службы Агента администрирования Kaspersky Security Center, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером\Службы.

### См. также:

Поддержка динамических виртуальных машин ..... 202

Просмотр Политики конфиденциальности ..... 216

## Установка Агента администрирования в неинтерактивном (тихом) режиме

Агент администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки. Для неинтерактивной установки используется инсталляционный пакет (MSI) Агента администрирования. MSI-файл расположен в дистрибутиве программы Kaspersky Security Center в папке Packages\NetAgent\exec.

► *Чтобы установить Агент администрирования на локальном устройстве в неинтерактивном режиме:*

1. Прочитайте Лицензионное соглашение (см. стр. 343). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. выполните команду

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PROP1=PROP1VAL PROP2=PROP2VAL`).

В список параметров вы должны включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Если вы используете стандартные параметры подключения для Kaspersky Security Center 11 и более поздних версий и Агента администрирования на удаленных устройствах, выполните команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` – ключ для записи в журнал событий. Журнал событий создается при установке Агента администрирования и сохраняется в папке C:\windows\temp\nag_inst.log.

Помимо nag_inst.log, программа создает файл $klssinstlib.log, который содержит журнал событий установки. Этот файл хранится в папке %windir%\temp or %temp%. Для устранения неполадок вам или специалисту Службы технической поддержки "Лаборатории Касперского" могут потребоваться оба файла журнала – nag_inst.log и $klssinstlib.log.

Если вам необходимо дополнительно указать порт для подключения к Серверу администрирования, введите команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com EULA=1
SERVERPORT=14000
```

Параметр `SERVERPORT` соответствует номеру порта подключения к Серверу администрирования.

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в неинтерактивном режиме, приведены в разделе Параметры установки Агента администрирования (см. стр. 199).

## См. также:



## Установка Агента администрирования для Linux в неинтерактивном (тихом) режиме (с файлом ответов)

Вы можете установить Агент администрирования на устройства с операционной системой Linux с помощью файла ответов – текстового файла, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом (неинтерактивном) режиме, то есть без участия пользователя.

► *Чтобы выполнить установку Агента администрирования для Linux в неинтерактивном режиме:*

1. Подготовьте требуемое устройство с операционной системой Linux для удаленной установки. Загрузите и создайте пакет удаленной установки, используя пакет Агента администрирования .deb или .rpm, с помощью любой подходящей системы управления пакетами.
2. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 387) и настройте Агент администрирования.
3. Прочитайте Лицензионное соглашение (см. стр. 343). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
4. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. Создайте файл ответов (в формате TXT) в каталоге, который вы указали в переменной среды. Добавьте в файл ответов список переменных в формате VARIABLE_NAME = variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вы должны включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В следующей таблице перечислены все переменные, которые можно включать в файл ответов:

   Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в неинтерактивном режиме
6. Установка Агента администрирования:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     ```
     # rpm -i klnagent-<build number>.i386.rpm
     ```
   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     ```
     # rpm -i klnagent64-<build number>.x86_64.rpm
     ```
   - Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
     ```
     # rpm -i klnagent64-<build number>.aarch64.rpm
     ```
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     ```
     # apt-get install ./klnagent_<build number>_i386.deb
     ```
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     ```
     # apt-get install ./klnagent64_<build number>_amd64.deb
     ```

- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<build number>_arm64.deb`

Установка Агента администрирования для Linux начинается в неинтерактивном режиме; пользователю не предлагается выполнять никаких действий во время процесса.

## Установка Kaspersky Security Center на Astra Linux в режиме замкнутой программной среды

В этом разделе описывается, как установить Агент администрирования для Linux на устройство с операционной системой Astra Linux Special Edition.

Перед установкой:

- Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования для Linux работает один из поддерживаемых дистрибутивов Linux (см. стр. 69).
- Загрузите ключ программы kaspersky_astra_pub_key.gpg https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.
- Загрузите необходимый установочный файл Агента администрирования с сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.

Выполните команды, представленные в этой инструкции, под учетной записью root.

► *Чтобы установить Агент администрирования для Linux на устройство с операционной системой Astra Linux Special Edition (обновление 1.7.2) и Astra Linux Special Edition (обновление 1.6):*

1. Откройте файл /etc/digsig/digsig_initramfs.conf и укажите следующие параметры:
   `DIGSIG_ELF_MODE=1`
2. В командной строке введите следующую команду, чтобы установить совместимый пакет:
   `apt install astra-digsig-oldkeys`
3. Создайте директорию для ключа программы:
   `mkdir -p /etc/digsig/keys/legacy/kaspersky/`
4. Поместите ключ программы в директории, созданной на предыдущем шаге:
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`
5. Обновите оперативную память дисков:
   `update-initramfs -u -k all`
6. Установка Агента администрирования:
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent_<build number>_i386.deb`
   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent64_<build number>_amd64.deb`

- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<build number>_arm64.deb`

Агент администрирования для Linux установлен.

## Локальная установка плагина управления программой

► *Чтобы установить плагин управления программой,*

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл klcfginst.exe, входящий в дистрибутивный пакет этой программы.

Файл klcfginst.exe входит в состав всех программ, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

## Установка программ в неинтерактивном режиме

► *Чтобы провести установку программы в неинтерактивном режиме:*

1. Откройте главное окно программы Kaspersky Security Center.
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужной программы или сформируйте для этой программы новый инсталляционный пакет.

   Инсталляционный пакет будет сохранен на Сервере администрирования в папке общего доступа в служебной папке Packages. При этом каждому инсталляционному пакету соответствует отдельная вложенная папка.

3. Откройте папку нужного инсталляционного пакета одним из следующих способов:
   - Скопируйте папку, соответствующую нужному инсталляционному пакету, с Сервера администрирования на клиентское устройство. Затем откройте скопированную папку на клиентском устройстве.
   - С клиентского устройства откройте на Сервере администрирования папку общего доступа, соответствующую нужному инсталляционному пакету.

   Если папка общего доступа расположена на устройстве с установленной операционной системой Microsoft Windows Vista, необходимо установить значение **Выключено** для параметра **Управление учетными записями пользователей: все администраторы работают в режиме одобрения администратором** (**Пуск → Панель управления → Администрирование → Локальная политика безопасности → Параметры безопасности**).

4. В зависимости от выбранной программы выполните следующие действия:
   - Для Антивируса Касперского для Windows Workstations, Антивируса Касперского для Windows Servers и Kaspersky Security Center перейдите во вложенную папку exec и запустите исполняемый файл (файл с расширением exe) с ключом /s.
   - Для остальных программ "Лаборатории Касперского" запустите из открытой папки исполняемый файл (файл с расширением exe) с ключом /s.

Запуск исполняемого файла с ключами EULA=1 и PRIVACYPOLICY=1 означает, что вы полностью прочитали, поняли и принимаете положения Лицензионного соглашения (см. стр. 343) и Политики конфиденциальности (см. стр. 216) соответственно. Вам также известно, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности. Текст Лицензионного соглашения и текст Политики конфиденциальности входят в комплект поставки Kaspersky Security Center. Согласие с положениями Лицензионного соглашения и Политики конфиденциальности является необходимым условием для установки программы или обновления предыдущей версии программы.

## Установка программ с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные инсталляционные пакеты программ. Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center.

► *Чтобы установить программу с помощью автономного инсталляционного пакета:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. В рабочей области выберите инсталляционный пакет нужной программы.
4. Запустите процесс создания автономного инсталляционного пакета одним из следующих способов:
   - в контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**;
   - по ссылке **Создать автономный пакет установки** в блоке работы с инсталляционным пакетом.

   В результате запускается мастер создания автономного инсталляционного пакета. Следуйте далее указаниям мастера.

   На завершающем шаге мастера выберите способ передачи автономного инсталляционного пакета на клиентское устройство.
5. Передайте автономный инсталляционный пакет программы на клиентское устройство.
6. Запустите автономный инсталляционный пакет на клиентском устройстве.

В результате программа будет установлена на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных инсталляционных пакетов используется порт 8060.

## Параметры инсталляционного пакета Агента администрирования

► *Чтобы настроить параметры инсталляционного пакета Агента администрирования:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета Агента администрирования.

**Общие**

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию программы, для которой сформирован инсталляционный пакет;
- размер инсталляционного пакета;
- дата создания инсталляционного пакета;
- путь к папке размещения инсталляционного пакета.

**Параметры**

В этом разделе можно настроить параметры, необходимые для обеспечения работоспособности Агента администрирования сразу после его установки. Параметры этого раздела доступны только для устройств под управлением Windows.

В блоке параметров **Папка установки** можно выбрать папку на клиентском устройстве, в которую будет установлен Агент администрирования:

- **Устанавливать в папку по умолчанию**

  Если выбран этот вариант, Агент администрирования будет установлен в папку <Диск>:\Program Files\Kaspersky Lab\NetworkAgent. Если такой папки нет, она будет создана автоматически.

  По умолчанию выбран этот вариант.

- **Устанавливать в заданную папку**

  Если выбран этот вариант, Агент администрирования будет установлен в папку, указанную в поле ввода.

В блоке параметров ниже можно задать пароль для задачи удаленной деинсталляции Агента администрирования:

- **Использовать пароль деинсталляции**

  Если параметр включен, при нажатии на кнопку **Изменить** можно ввести пароль для удаления программы (доступно только для Агента администрирования на устройствах под управлением операционных систем семейства Windows).

  По умолчанию параметр выключен.

- **Статус**

  Состояние пароля: **Пароль установлен** или **Пароль не установлен**.

По умолчанию пароль не установлен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без необходимых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

  Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

  По умолчанию параметр выключен.

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**

  Если этот параметр включен, все загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера мобильных устройств Exchange и Сервера iOS MDM будут установлены автоматически.

  Если этот параметр выключен, то загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

  По умолчанию параметр включен.

**Подключение**

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования:

В этом разделе можно настроить параметры подключения Агента администрирования к Серверу администрирования. Для установления соединения можно использовать SSL-протокол или UDP-протокол. Для настройки соединения укажите следующие параметры:

- **Адрес SMTP-сервера**

  Адрес устройства, на котором установлен Сервер администрирования.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

  Номер порта, по которому будет выполняться подключение с использованием протокола SSL.

- **Использовать сертификат Сервера**

  Если этот параметр включен, для аутентификации доступа Агента администрирования к Серверу администрирования будет использоваться файл сертификата, который можно указать при нажатии на кнопку **Обзор**.

  Если этот параметр выключен, файл сертификата будет получен с Сервера администрирования при первом подключении Агента администрирования по адресу, указанному в поле **Адрес сервера**.

  Не рекомендуется выключать параметр, так как автоматическое получение сертификата Сервера администрирования Агентом администрирования при

подключении к Серверу является небезопасным.

По умолчанию флажок установлен.

- **Использовать SSL**

  Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию параметр выключен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- **Использовать UDP-порт**

  Если этот параметр включен, подключение Агента администрирования к Серверу администрирования будет выполняться через UDP-порт. Это позволяет управлять клиентскими устройствами и получать информацию о них.

  UPD-порт должен быть открыт на управляемых устройствах, на которых установлен Агент администрирования. Поэтому рекомендуется не выключать этот параметр.

  По умолчанию параметр включен.

- **Номер UDP-порта**

  В поле можно указать номер порта подключения Агента администрирования к Серверу администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если параметр включен, после установки Агента администрирования на клиентском устройстве в список исключений брандмауэра Microsoft Windows будет добавлен UDP-порт. Этот UDP-порт требуется для корректной работы Агента администрирования.

  По умолчанию параметр включен.

**Дополнительно**

В разделе **Дополнительно**, вы можете настроить, как использовать шлюз соединения. Для этого можно выполнить следующие действия:

- Используйте Агент администрирования в качестве шлюза соединения в демилитаризованной зоне (DMZ) для подключения к Серверу администрирования, связи с ним и сохранения данных в безопасности на Агенте администрирования (см. стр. 90), во время передачи данных.
- Подключайтесь к Серверу администрирования с помощью шлюза соединения, чтобы уменьшить количество подключений к Серверу администрирования. В этом случае введите адрес устройства, которое будет выступать в качестве шлюза соединения в поле **Адрес шлюза соединения**.
- Настройте подключение для Virtual Desktop Infrastructure (VDI), если в вашей сети есть виртуальные машины. Для этого выполните следующее:
  - **Включить динамический режим для VDI**

    Если параметр включен, для Агента администрирования, установленного на виртуальной машине, будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

    По умолчанию параметр выключен.

  - **Оптимизировать параметры для VDI**

Если параметр включен, в параметрах Агента администрирования выключены следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

По умолчанию параметр выключен.

**Дополнительные компоненты**

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

**Теги**

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

**История ревизий**

В этом разделе можно посмотреть историю ревизий инсталляционного пакета (см. стр. 811). Вы можете сравнивать ревизии, просматривать ревизии, сохранять ревизии в файл, добавлять и изменять описания ревизий.

Параметры инсталляционного пакета Агента администрирования доступны для конкретной операционной системы, которые приведены в таблице ниже.

*Таблица 42. Параметры инсталляционного пакета Агента администрирования*

| Раздел свойств | Windows | Mac | Linux |
|---|---|---|---|
| **Общие** | ✓ | ✓ | ✓ |
| **Параметры** | ✓ | — | — |
| **Подключение** | ✓ | ✓ (за исключением параметров **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** и **Использовать только автоматическое определение прокси-сервера**) | ✓ (за исключением параметров **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** и **Использовать только автоматическое определение прокси-сервера**) |
| **Дополнительно** | ✓ | ✓ | ✓ |
| **Дополнительные компоненты** | ✓ | ✓ | ✓ |
| **Теги** | ✓ | ✓ (кроме правил автоматического назначения тегов) | ✓ (кроме правил автоматического назначения тегов) |
| **История ревизий** | ✓ | ✓ | ✓ |

## Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице https://www.kaspersky.ru/products-and-services-privacy-policy; также она доступна в офлайн-режиме. Вы можете ознакомиться с Политикой конфиденциальности, например, перед установкой Агента администрирования.

► *Чтобы прочитать Политику конфиденциальности в офлайн-режиме:*

1. Запустите установщик Kaspersky Security Center.
2. В окне установщика перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В открывшемся списке выберите Агент администрирования Kaspersky Security Center и нажмите на кнопку **Далее**.

Файл privacy_policy.txt появится на вашем устройстве в указанной вами папке в подпапке NetAgent.

kaspersky

# Установка Kaspersky Security Center

В этом разделе описывается установка компонентов Kaspersky Security Center. Если вы хотите установить программу локально только на одно устройство, доступны два варианта установки:

- **Стандартная**. Этот вариант рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Также вы можете установить только набор модулей управления, заданный по умолчанию, для программ "Лаборатории Касперского". Вы также можете воспользоваться стандартной установкой, если вы уже имеете опыт работы с Kaspersky Security Center и знаете, как после стандартной установки настроить все необходимые вам параметры.
- **Выборочная**. Этот вариант рекомендуется, если вы планируете настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При необходимости вы можете запустить выборочную установку в неинтерактивном режиме (см. стр. 270).

Если в сети установлен хотя бы один Сервер администрирования, Серверы на других устройствах сети могут быть установлены с помощью задачи удаленной установки методом принудительной установки (см. стр. 361). При создании задачи удаленной установки программы необходимо использовать инсталляционный пакет Сервера администрирования: ksc_<номер_версии>.<номер сборки>_full_<язык локализации>.exe.

Используйте этот пакет, если вы хотите установить все компоненты, необходимые для работы всех функций Kaspersky Security Center, или обновить существующие версии этих компонентов.

Если хотите развернуть отказоустойчивый кластер "Лаборатории Касперского" (см. стр. 253), вам необходимо установить Kaspersky Security Center на все узлы кластера.

## См. также:



## В этом разделе

kaspersky

## Подготовка к установке

Выполните следующие действия перед запуском установки.

- Проверка требований к оборудованию и программному обеспечению

  Убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям, предъявляемым к Серверу администрирования и Консоли администрирования (см. стр. 69).

- Выбор и установка системы управления базами данных (СУБД)

  Kaspersky Security Center хранит свою информацию в базе данных, управляемой СУБД. Установите СУБД в сети до установки Kaspersky Security Center (узнайте больше о том, как выбрать СУБД). Если вы решили установить СУБД PostgreSQL или Postgres Pro, укажите пароль для суперпользователя. Если пароль не указан, Сервер администрирования может не подключиться к базе данных.

  Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

  Установите Сервер администрирования, Агент администрирования и Консоль администрирования в папках, в которых выключен учет регистра. Также необходимо выключить учет регистра для общей папки Сервера администрирования и скрытой папки Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

  Вместе с компонентом Сервер администрирования на устройство будет установлена серверная версия Агента администрирования. Его совместная установка с обычной версией Агента администрирования невозможна. Если серверная версия Агента администрирования уже установлена на вашем устройстве, требуется удалить ее и запустить установку Сервера администрирования повторно. Подробнее о серверной версии Агента администрирования см. раздел Изменения в системе после установки Kaspersky Security Center (см. стр. 277).

- Проверка учетных записей

  Для установки Kaspersky Security Center необходимо наличие прав локального администратора на устройстве, где осуществляется установка.

  Kaspersky Security Center поддерживает управляемые учетные записи службы и групповые управляемые учетные записи службы. Если эти типы учетных записей используются в вашем домене и вы хотите указать одну из них в качестве учетной записи для службы Сервера администрирования, то сначала установите учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

## Учетные записи для работы с СУБД

Для установки Сервера администрирования и работы с ним вам потребуется учетная запись Windows, под которой вы будете запускать программу установки Сервера администрирования (далее также "инсталлятор"), учетная запись Windows, под которой вы будете запускать службу Сервера администрирования, и внутренняя учетная запись СУБД для доступа к СУБД. Можно создать учетные записи или использовать существующие. Все эти учетные записи требуют определенных прав. Набор необходимых учетных записей и их права зависят от следующих критериев:

- Тип СУБД:
  - Microsoft SQL Server (с аутентификацией Windows или с аутентификацией SQL Server);
  - MySQL или MariaDB
  - PostgreSQL или Postgres Pro
- Расположение СУБД:
  - **Локальная СУБД**. *Локальной СУБД* называется СУБД, установленная на том же устройстве, что и Сервер администрирования.
  - **Удаленная СУБД**. *Удаленной СУБД* называется СУБД, установленная на другом устройстве.
- Способ создания базы данных Сервера администрирования:
  - **Автоматически**. При установке Сервера администрирования вы можете автоматически создать базу данных Сервера администрирования (далее также база данных Сервера) с помощью инсталлятора.
  - **Вручную**. Можно использовать программу стороннего производителя (например, SQL Server Management Studio) или скрипт для создания пустой базы данных. После этого вы можете указать эту базу данных в качестве базы данных Сервера при установке Сервера администрирования.

При предоставлении прав и разрешений учетным записям соблюдайте принцип наименьших привилегий. Это означает, что предоставленных прав достаточно только для выполнения требуемых действий.

В приведенных ниже таблицах содержится информация о системных правах и правах на СУБД, которые требуется предоставить учетным записям перед установкой и запуском Сервера администрирования.

#### Microsoft SQL Server с аутентификацией Windows

Если вы выбираете SQL Server в качестве СУБД, можно использовать аутентификацию Windows для доступа к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска программы установки, и для учетной записи Windows, используемой для запуска службы Сервера администрирования. В SQL Server создайте учетные записи для этих учетных записей Windows. В зависимости от метода создания базы данных Сервера предоставьте необходимые права SQL Server этим учетным записям, как описано в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация Windows) (см. стр. 225).

*Таблица 43. СУБД: Microsoft SQL Server (в том числе и Express Edition) с аутентификацией Windows*

| | Автоматическое создание базы данных (программой установки) | Создание базы данных вручную (администратором) |
|---|---|---|
| **Учетная запись, от имени которой работает инсталлятор** | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. |
| **Права учетной записи, от имени которой работает инсталлятор** | • Системные права: права локального администратора.<br>• Права SQL Server:<br>Роль уровня сервера: sysadmin. | • Системные права: права локального администратора.<br>• Права SQL Server:<br>Роль уровня сервера: public.<br>Роль членства базы данных для базы данных Сервера: db_owner, public.<br>Схема по умолчанию для базы данных Сервера: dbo. |
| **Учетная запись службы Сервера администрирования.** | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую создает программа установки автоматически (в этом случае не рекомендуется создавать учетную запись KL-AK-* (см. стр. 225). |
| **Права учетной записи службы Сервера администрирования** | • Системные права: необходимые права, присвоенные инсталлятором.<br>• Права SQL Server: необходимые права, присвоенные инсталлятором. | • Системные права: необходимые права, присвоенные инсталлятором.<br>• Права SQL Server:<br>Роль уровня сервера: public.<br>Роль членства базы данных для базы данных Сервера: db_owner, public.<br>Схема по умолчанию для базы данных Сервера: dbo. |

**Microsoft SQL Server с аутентификацией SQL Server**

Если вы выбираете SQL Server в качестве СУБД, вы можете использовать аутентификацию SQL Server для подключения к SQL Server. Настройте системные права для учетной записи Windows, используемой для запуска программы установки, и для учетной записи Windows, используемой для работы с Сервером администрирования. В SQL Server создайте учетную запись с паролем, чтобы использовать это для аутентификации. Затем предоставьте этой учетной записи SQL Server необходимые права, перечисленные в таблице ниже. Подробнее о настройке прав учетных записей см. раздел Настройка учетных записей для работы с SQL Server (аутентификация SQL Server)(см. стр. 227).

Таблица 44. СУБД: Microsoft SQL Server (в том числе и Express Edition) с аутентификацией SQL Server

| | Автоматическое создание базы данных (программой установки) | Создание базы данных вручную (администратором) |
|---|---|---|
| **Учетная запись, от имени которой работает инсталлятор** | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. |
| **Права учетной записи, от имени которой работает инсталлятор** | Системные права: права локального администратора. | Системные права: права локального администратора. |
| **Учетная запись службы Сервера администрирования.** | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. | • Удаленная СУБД: только доменная учетная запись удаленного устройства, на котором установлена СУБД.<br>• Локальная СУБД:<br>Учетная запись пользователя Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. |
| **Права учетной записи службы Сервера администрирования** | Системные права: необходимые права, присвоенные инсталлятором. | Системные права: необходимые права, присвоенные инсталлятором. |

| | Автоматическое создание базы данных (программой установки) | Создание базы данных вручную (администратором) |
|---|---|---|
| **Права учетной записи, используемой для аутентификации SQL Server** | Права SQL Server, необходимые для создания базы данных и установки Сервера администрирования:<br>• Роль уровня сервера: public.<br>• Роль членства базы данных для базы данных *master*: db_owner.<br>• Схема по умолчанию для базы данных *master*: dbo.<br>• Разрешения:<br>CONNECT ANY DATABASE<br>CONNECT SQL<br>CREATE ANY DATABASE<br>VIEW ANY DATABASE<br>Права SQL Server, необходимые для работы с Сервером администрирования:<br>• Роль уровня сервера: public.<br>• Роль членства базы данных для базы данных Сервера: db_owner.<br>• Схема по умолчанию для базы данных Сервера: dbo.<br>• Разрешения:<br>CONNECT SQL<br>VIEW ANY DATABASE | Права SQL Server:<br>• Роль уровня сервера: public.<br>• Роль членства базы данных для базы данных Сервера: db_owner.<br>• Схема по умолчанию для базы данных Сервера: dbo.<br>• Разрешения:<br>CONNECT SQL<br>VIEW ANY DATABASE |

**Настройка прав SQL Server для восстановления данных Сервера администрирования**

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования. Перед запуском утилиты klbackup на SQL Server предоставьте права для входа в SQL Server, связанного с этой учетной записью Windows. Права SQL Server различаются в зависимости от версии Сервера администрирования. Для Сервера администрирования версии 14.2 и выше можно назначить серверную роль sysadmin или серверную роль dbcreator.

*Таблица 45. Права SQL Server для восстановления базы данных Сервера администрирования*

| Сервер администрирования версии 14.2 и выше | Другие версии Сервера администрирования |
|---|---|
| • Права SQL Server:<br>Роль уровня сервера: sysadmin. | • Права SQL Server:<br>Роль уровня сервера: sysadmin. |
| • Права SQL Server:<br>Роль уровня сервера: dbcreator.<br>• Разрешения:<br>VIEW ANY DEFINITION<br>Перед запуском утилиты klbackup укажите флаг сервера KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Для этого выполните следующую команду в командной строке:<br>`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1` | |

**MySQL и MariaDB**

Если вы выбираете MySQL или MariaDB в качестве СУБД, создайте внутреннюю учетную запись СУБД и предоставьте этой учетной записи необходимые права, перечисленные в таблице ниже. Программа установки и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Обратите внимание, что способ создания базы данных не влияет на набор необходимых прав. Подробнее о настройке прав учетной записи см. раздел Настройка учетных записей для работы с MySQL и MariaDB (см. стр. 230).

*Таблица 46. СУБД: MySQL и MariaDB*

| | Автоматическое или ручное создание базы данных |
|---|---|
| **Учетная запись, от имени которой работает инсталлятор** | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. |
| **Права учетной записи, от имени которой работает инсталлятор** | Системные права: права локального администратора. |
| **Учетная запись службы Сервера администрирования.** | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. |
| **Права учетной записи службы Сервера администрирования** | Системные права: требуемые права, присвоенные инсталлятором. |

| | Автоматическое или ручное создание базы данных |
|---|---|
| **Права внутренней учетной записи СУБД** | Схема привилегий:<br>• База данных Сервера администрирования: ALL (кроме GRANT OPTION).<br>• Схемы системы (mysql и sys): SELECT, SHOW VIEW.<br>• Хранимая процедура sys.table_exists: EXECUTE (если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE).<br>Глобальные привилегии для всех схем: PROCESS, SUPER. |

**Настройка прав на восстановление данных Сервера администрирования**

Прав, которые вы предоставили для внутренней учетной записи СУБД, достаточно для восстановления данных Сервера администрирования из резервной копии. Чтобы начать восстановление, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования.

**PostgreSQL или Postgres Pro**

Если вы выбираете PostgreSQL или Postgres Pro в качестве СУБД, вы можете использовать пользователя *Postgres* (роль Postgres по умолчанию) или создать роль Postgres (далее также роль) для доступа к СУБД. В зависимости от способа создания базы данных Сервера предоставьте необходимые права роли, как описано в таблице ниже. Подробнее о настройке прав роли см. раздел Настройка учетных записей для работы с PostgreSQL или Postgres Pro (см. стр. 232).

*Таблица 47. СУБД: PostgreSQL или Postgres Pro*

| | Автоматическое создание базы данных | Создание базы данных вручную |
|---|---|---|
| **Учетная запись, от имени которой работает инсталлятор** | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД: учетная запись локального администратора или учетная запись домена. |
| **Права учетной записи, от имени которой работает инсталлятор** | Системные права: права локального администратора. | Системные права: права локального администратора. |
| **Учетная запись службы Сервера администрирования.** | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором. | • Удаленная СУБД: только доменная учетная запись удаленного устройства с установленной СУБД.<br>• Локальная СУБД:<br>Учетная запись Windows, выбранная администратором.<br>Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. |

| | Автоматическое создание базы данных | | Создание базы данных вручную |
|---|---|---|---|
| | Учетная запись в формате KL-AK-*, которую программа установки создает автоматически. | | |
| **Права учетной записи службы Сервера администрирования** | Системные права: требуемые права, присвоенные инсталлятором. | | Системные права: требуемые права, присвоенные инсталлятором. |
| **Права роли Postgres** | Пользователю *Postgres* не требуются дополнительные права. | Права для новой роли: `CREATEDB`. | Для новой роли:<br>• Права доступа к базе данных Сервера администрирования: `ALL`.<br>• Права для всех таблиц в общедоступной схеме: `ALL`.<br>• Права доступа ко всем последовательностям в общедоступной схеме: `ALL`. |

**Настройка прав на восстановление данных Сервера администрирования**

Чтобы восстановить данные Сервера администрирования из резервной копии, запустите утилиту klbackup под учетной записью Windows, под которой был установлен Сервер администрирования. Обратите внимание, что роль Postgres, используемая для доступа к СУБД, должна иметь права владельца на базу данных Сервера администрирования.

См. также:

Основной сценарий установки.....92

## Настройка учетных записей для работы с SQL Server (аутентификация Windows)

**Предварительные требования**

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.
5. В SQL Server создайте учетную запись для учетной записи Windows, используемой для запуска программы установки Сервера администрирования (далее также "инсталлятор"). Также создайте учетную запись Windows, используемую для запуска службы Сервера администрирования.

Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация Windows**.

Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе Учетные записи для работы с СУБД (см. стр. 218).

**Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)**

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. В SQL Server назначьте роль sysadmin на уровне сервера для учетной записи Windows, которая используется для запуска программы установки.
2. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
3. Запустите программу установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования (см. стр. 243).
5. Выберите Microsoft SQL Server как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
6. Выберите Режим аутентификации Microsoft Windows (см. стр. 248), чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.
7. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

   Можно выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись SQL Server. Кроме того, вы можете автоматически создать учетную запись Windows в формате KL-AK-* с помощью программы установки. В этом случае программа установки автоматически создает для этой учетной записи учетную запись для SQL Server. Независимо от выбора учетной записи программа установки назначает необходимые системные права и права SQL Server учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права и права SQL Server назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

**Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)**

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования (далее также база данных Сервера).
2. Для обоих учетных записей SQL Server, созданных для учетных записей Windows, укажите общедоступную роль уровня сервера и настройте сопоставление с созданной базой данных:
   - Роль уровня сервера: public.
   - Роль членства базы данных: db_owner, public.
   - Схема по умолчанию: dbo.

3. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
4. Запустите программу установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
5. Выберите выборочную установку Сервера администрирования (см. стр. 243).
6. Выберите Microsoft SQL Server как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования (см. стр. 247).
8. Выберите Режим аутентификации Microsoft Windows (см. стр. 248), чтобы установить соединение между Сервером администрирования и SQL Server с помощью учетной записи Windows.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

   Вы можете выбрать учетную запись пользователя Windows, для которой вы ранее создали учетную запись входа в SQL Server и настроили права входа.

Не рекомендуется автоматически создавать учетную запись Windows в формате KL-AK-*. В этом случае программа установки создает учетную запись Windows, для которой вы не создали и не настроили учетную запись SQL Server. Сервер администрирования не может использовать эту учетную запись для запуска службы Сервера администрирования. Если необходимо создать учетную запись KL-AK-* Windows, не запускайте Консоль администрирования после установки. Вместо этого сделайте следующее:

1. Остановите службу kladminserver.
2. В SQL Server создайте учетную запись SQL Server для созданной учетной записи KL-AK-* Windows.
3. Предоставьте права этой учетной записи SQL Server и настройте сопоставление с созданной базой данных:
   - Роль уровня сервера: public.
   - Роль членства базы данных: db_owner, public.
   - Схема по умолчанию: dbo.
4. Перезапустите службу kladminserver, а затем запустите Консоль администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера. Сервер администрирования готов к работе.

## Настройка учетных записей для работы с SQL Server (аутентификация SQL Server)

### Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с SQL Server.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

5. В SQL Server включите режим аутентификации SQL Server.

   Если вы используете SQL Server Management Studio, в окне свойств SQL Server на странице **Безопасность** выберите параметр **SQL Server и режим аутентификации Windows**.

6. В SQL Server создайте учетную запись с паролем. Программа установки Сервера администрирования (программа установки) и служба Сервера администрирования используют эту учетную запись SQL Server для доступа к SQL Server.

   Если вы используете SQL Server Management Studio, на странице **Общие** окна свойств входа выберите параметр **Аутентификация SQL-сервера**.

Если вы хотите установить Сервер администрирования и SQL Server на устройства, расположенные в разных доменах Windows, обратите внимание, что эти домены должны иметь двусторонние отношения доверия, чтобы обеспечить корректную работу Сервера администрирования, включая выполнение задач и применение политик. Информацию о необходимых учетных записях для работы с различными СУБД и правах учетных записей см. в разделе Учетные записи для работы с СУБД (см. стр. 218).

**Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)**

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. В SQL Server сопоставьте учетную запись SQL Server с учетной записью по умолчанию в базе данных *master*. База данных *master* является шаблоном для базы данных Сервера администрирования (далее также база данных Сервера). База данных *master* используется для сопоставления до тех пор, пока программа установки не создаст базу данных Сервера. Предоставьте следующие права и разрешения учетной записи SQL Server:
   - Роль уровня сервера: public.
   - Роль членства базы данных для *мастер* базы данных: db_owner.
   - Схема по умолчанию для базы данных *master*: dbo.
   - Разрешения:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
3. Запустите программу установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
4. Выберите выборочную установку Сервера администрирования (см. стр. 243).
5. Выберите Microsoft SQL Server как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
6. Укажите имя базы данных Сервера администрирования (см. стр. 247).

7. Выберите режим аутентификации SQL Server (см. стр. 248), чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.
8. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

   Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью программы установки. Независимо от выбранной учетной записи программа установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера и все необходимые системные права назначаются учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

Вы можете отменить привязку к базе данных *master*, так как программа установки создала базу данных Сервера и настроила сопоставление с этой базой данных при установке Сервера администрирования.

Так как для автоматического создания базы данных требуется больше разрешений, чем для ежедневной работы с Сервером администрирования, вы можете отозвать некоторые разрешения. На SQL Server выберите учетную запись SQL Server и предоставьте следующие права для работы с Сервером администрирования:

- Роль уровня сервера: public.
- Роль членства базы данных для базы данных Сервера: db_owner.
- Схема по умолчанию для базы данных Сервера: dbo.
- Разрешения:
  - CONNECT SQL
  - VIEW ANY DATABASE

**Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)**

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. На SQL Server создайте пустую базу данных. Эта база данных будет использоваться в качестве базы данных Сервера администрирования.
2. В SQL Server предоставьте следующие права и разрешения учетной записи SQL Server:
   - Роль уровня сервера: public.
   - Роль членства базы данных для создания базы данных: db_owner.
   - Схема по умолчанию для создания базы данных: dbo.
   - Разрешения:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
4. Запустите программу установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

5. Выберите выборочную установку Сервера администрирования (см. стр. 243).
6. Выберите Microsoft SQL Server как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
7. Укажите имя созданной базы данных в качестве имени базы данных Сервера администрирования (см. стр. 247).
8. Выберите режим аутентификации SQL Server (см. стр. 248), чтобы установить соединение между Сервером администрирования и SQL Server с помощью созданной учетной записью SQL Server. Затем укажите данные учетной записи SQL Server.
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

   Вы можете выбрать существующую учетную запись пользователя Windows или создать учетную запись Windows в формате KL-AK-* с помощью программы установки. Независимо от выбранной учетной записи программа установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Все необходимые системные права назначены учетной записи службы Сервера администрирования. Сервер администрирования готов к работе.

## Настройка учетных записей для работы с MySQL и MariaDB

### Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с MySQL или MariaDB.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

### Настройка учетных записей для установки Сервера администрирования

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. Запустите среду для работы с MySQL или MariaDB под учетной записью root, которую вы создали при установке СУБД.
2. Создайте внутреннюю учетную запись СУБД с паролем. Программа установки Сервера администрирования (далее также программа установки) и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД. Предоставьте этой учетной записи следующие права:
   - Схема привилегий:
     - База данных Сервера администрирования: ALL (кроме `GRANT OPTION`).
     - Схемы системы (mysql и sys): `SELECT`, `SHOW VIEW`.
     - Хранимая процедура sys.table_exists: `EXECUTE`
   - Глобальные привилегии для всех схем: `PROCESS`, `SUPER`.

Чтобы создать внутреннюю учетную запись СУБД и предоставить этой учетной записи необходимые права, запустите приведенный ниже скрипт (в этом скрипте учетная запись СУБД – *KCSAdmin*, а имя базы данных Сервера администрирования – *kav*):

```
/* Создать пользователя с именем KSCAdmin */
CREATE USER 'KSCAdmin'
/* Указать пароль для KSCAdmin */
IDENTIFIED BY '<пароль>';
/* Предоставить привилегии KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

> Если вы используете MariaDB 10.5 или более раннюю версию в качестве СУБД, вам не нужно предоставлять право EXECUTE. В этом случае исключите из скрипта следующую команду: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'.`

3. Чтобы просмотреть список привилегий, предоставленных учетной записи СУБД, запустите следующий скрипт:

   ```
   SHOW предоставляет для 'KSCAdmin'
   ```

4. Чтобы вручную создать базу данных Сервера администрирования, запустите следующий скрипт (в этом скрипте имя базы данных Сервера администрирования – *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET 'ascii'
   COLLATE 'ascii_general_ci';
   ```

   Используйте то же имя базы данных, которое вы указали в сценарии, создающем учетную запись СУБД.

5. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
6. Запустите программу установки.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

7. Выберите выборочную установку Сервера администрирования (см. стр. 243).
8. Выберите MySQL или MariaDB как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
9. Укажите имя базы данных Сервера администрирования (см. стр. 247). Используйте то же имя базы данных, которое вы указали в скрипте.
10. Укажите учетные данные учетной записи СУБД (см. стр. 248), которую вы создали с помощью скрипта.

11. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

    Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью программы установки. Независимо от выбранной учетной записи программа установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки создается база данных Сервера администрирования и Сервер администрирования готов к работе.

## См. также:

Сценарий:Управление программами .....556

## Настройка учетных записей для работы с PostgreSQL и Postgres Pro

### Предварительные требования

Прежде чем назначать права учетным записям, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с PostgreSQL и Postgres Pro.
3. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете устанавливать Сервер администрирования.
4. Убедитесь, что у вас есть учетная запись Windows, под которой вы будете запускать службу Сервера администрирования.

### Настройка учетных записей для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. Запустите среду для работы с PostgreSQL и Postgres Pro.
2. Выберите роль Postgres для доступа к СУБД. Вы можете использовать одну из следующих ролей:
   - Пользователь *Postgres* (роль Postgres по умолчанию).

     Если вы используете пользователя *Postgres*, предоставлять ему дополнительные права не требуется.
   - Новая роль Postgres.

     Если вы хотите использовать новую роль Postgres, создайте эту роль и предоставьте ей право CREATEDB. Для этого запустите следующий скрипт (в этом скрипте роль имеет значение *KCSAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<пароль>' CREATEDB;
     ```

     Созданная роль будет использоваться в качестве владельца базы данных Сервера администрирования (далее также база данных Сервера).
3. Войдите в систему под учетной записью Windows, под которой был запущена программа установки Сервера администрирования (далее также инсталлятор).
4. Запустите программу установки.

Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

5. Выберите выборочную установку Сервера администрирования (см. стр. 243).
6. Выберите PostgreSQL или Postgres Pro как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.
7. Укажите имя базы данных Сервера (см. стр. 247). Программа установки автоматически создаст базу данных Сервера.
8. Укажите учетные данные роли Postgres (см. стр. 248).
9. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

   Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью программы установки. Независимо от выбранной учетной записи программа установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки автоматически создается база данных Сервера, и Сервер администрирования готов к работе.

**Настройка учетных записей для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)**

► *Чтобы настроить учетные записи для установки Сервера администрирования:*

1. Запустите среду для работы с Postgres.
2. Создайте роль Postgres и базу данных Сервера администрирования. Затем предоставьте роли все права в базе данных Сервера администрирования. Для этого выполните вход под пользователем *Postgres* в базу данных *Postgres* и запустите следующий скрипт (в этом скрипте роль имеет значение *KCSAdmin*, а имя базы данных Сервера администрирования – *KAV*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<пароль>';
   CREATE DATABASE "KAV" ENCODING 'UTF8';
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

3. Предоставьте следующие права созданной роли Postgres:

   - Права для всех таблиц в общедоступной схеме: ALL.
   - Права доступа ко всем последовательностям в общедоступной схеме: ALL.

   Для этого выполните вход под пользователем *Postgres* в базу данных Сервера и запустите следующий скрипт (в этом скрипте роль имеет значение *KCSAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

4. Войдите в систему под учетной записью Windows, используемой для запуска программы установки.
5. Запустите программу установки Сервера администрирования.

   Запустится мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

6. Выберите выборочную установку Сервера администрирования (см. стр. 243).
7. Выберите PostgreSQL или Postgres Pro как СУБД (см. стр. 246), в которой хранится база данных Сервера администрирования.

8. Укажите имя базы данных Сервера (см. стр. 247). Используйте то же имя базы данных, которое вы указали в скрипте. Учитывайте регистр при вводе имени базы данных.
9. Укажите учетные данные роли Postgres (см. стр. 248).
10. Укажите учетную запись Windows, которая используется для запуска службы Сервера администрирования (см. стр. 249).

    Вы можете выбрать существующую учетную запись пользователя Windows или автоматически создать учетную запись Windows в формате KL-AK-* с помощью программы установки. Независимо от выбранной учетной записи программа установки назначает необходимые системные права учетной записи службы Сервера администрирования.

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Сервер администрирования готов к работе.

## Сценарий: Аутентификация Microsoft SQL Server

Информация в этом разделе применима только к конфигурациям, в которых Kaspersky Security Center использует Microsoft SQL Server в качестве системы управления базами данных.

Чтобы защитить данные Kaspersky Security Center, передаваемые в базу данных или из нее, а также данные, хранящиеся в базе данных, от несанкционированного доступа, вы должны защитить связь между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь - это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обеих программ. Во всех других случаях мы рекомендуем использовать сертификат SSL или TLS для аутентификации экземпляра SQL Server. Вы можете использовать сертификат аккредитованного центра сертификации (CA) или самоподписанный сертификат. Рекомендуется использовать сертификат аккредитованного центра сертификации, так как самоподписанный сертификат обеспечивает лишь ограниченную защиту.

Аутентификация SQL Server состоит из следующих этапов:

a. **Создание самоподписанного сертификата SSL или TLS для SQL Server в соответствии с требованиями сертификата https://docs.microsoft.com/ru-RU/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017#certificate-requirements**

Если у вас уже есть сертификат для SQL Server, пропустите этот шаг.

SSL-сертификат можно применять только к версиям SQL Server ранее 2016 года (13.x). В версиях SQL Server 2016 (13.x) и выше используйте TLS-сертификат.

Например, чтобы создать TLS-сертификат, введите следующую команду в PowerShell:

```
New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert: \ LocalMachine -KeySpec KeyExchange
```

В командной строке в качестве SQL_HOST_NAME вы должны ввести имя экземпляра SQL Server, если экземпляр включен в домен, или ввести *полное доменное имя* (FQDN) экземпляра, если экземпляр не включен в домен. В мастере установки Сервера администрирования (см. стр. 247) в качестве имени экземпляра SQL Server должно быть указано то же имя – имя экземпляра или полное доменное имя.

**b. Добавление сертификата на экземпляр SQL Server**

Инструкции этого этапа зависят от платформы, на которой работает SQL Server. Дополнительную информацию см. в официальной документации:

Windows https://docs.microsoft.com/ru-ru/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017

Linux https://docs.microsoft.comr/ru-ru/sql/linux/sql-server-linux-encrypted-connections?view=sql-server-2017

служба реляционных баз данных Amazon https://docs.aws.amazon.com/en_us/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html

Windows Azure https://azure.microsoft.com/ru-ru/blog/windows-azure-root-certificate-migration/

Чтобы использовать сертификат в отказоустойчивом кластере, необходимо установить сертификат на каждом узле отказоустойчивого кластера. Подробнее см. документацию Microsoft https://docs.microsoft.com/ru-RU/sql/database-engine/configure-windows/manage-certificates?view=sql-server-2017.

**c. Назначение разрешений для учетной записи службы**

Убедитесь, что учетная запись службы, под которой запускается служба SQL Server, имеет разрешения "Полный доступ" для доступа к закрытым ключам. Подробнее см. документацию Microsoft https://docs.microsoft.com/ru-RU/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-2017#to-provision-install-a-certificate-on-a-single-server.

**d. Добавление сертификата в список доверенных сертификатов для Kaspersky Security Center**

На устройство Сервера администрирования добавьте сертификат в список доверенных сертификатов. Подробнее см. документацию Microsoft https://docs.microsoft.com/ru-RU/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.

**e. Включение зашифрованных подключений между экземпляром SQL Server и Kaspersky Security Center**

На устройстве Сервера администрирования установите значение `1` для переменной среды `KLDBADO_UseEncryption`. Например, в Windows Server 2012 R2 вы можете изменить переменные среды, нажав на **Переменные среды**, на закладке **Дополнительно** окна **Свойства системы**. Добавьте переменную с именем `KLDBADO_UseEncryption` и установите значение `1`.

**f. Дополнительная настройка для использования TLS-протокола 1.2**

Если вы используете TLS-протокол 1.2, дополнительно выполните следующие действия:

Убедитесь, что установленная версия SQL Server является 64-разрядной программой.

Установите драйвер Microsoft OLE DB на устройство Сервера администрирования. Подробнее см. документацию Microsoft https://docs.microsoft.com/ru-RU/sql/connect/oledb/oledb-driver-for-sql-server?view=sql-server-2017.

На устройстве Сервера администрирования установите значение `1` для переменной среды `KLDBADO_UseMSOLEDBSQL`. Например, в Windows Server 2012 R2 вы можете изменить переменные среды, нажав на **Переменные среды**, на закладке **Дополнительно** окна **Свойства системы**. Добавьте новую переменную с именем `KLDBADO_UseMSOLEDBSQL` и установите значение `1`.

Если версия драйвера OLE DB – 19 или выше, также установите значение `MSOLEDBSQL19` в переменную окружения `KLDBADO_ProviderName`.

**g. Включение использования протокола TCP/IP на именованном экземпляре SQL Server**

Если вы используете именованный экземпляр SQL Server, дополнительно включите использование протокола TCP/IP https://docs.microsoft.com/ru-RU/sql/database-engine/configure-windows/enable-or-disable-a-server-network-protocol?view=sql-server-ver15 и назначьте номер порта TCP/IP https://docs.microsoft.com/ru-RU/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver15 для компонента SQL Server Database Engine. При настройке подключения к SQL Server в мастере установки Сервера администрирования (см. стр. 247) укажите имя экземпляра SQL Server и номер порта в поле **Имя экземпляра SQL Server**.

kaspersky

# Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

## См. также:



## В этом разделе



## Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

По умолчанию инсталлятор самостоятельно создает непривилегированные учетные записи для служб Сервера администрирования. Такое поведение наилучшим образом подходит для установки Сервера администрирования на обычное устройство.

Однако при установке Сервера администрирования на отказоустойчивый кластер следует поступить иначе:

1. Создать непривилегированные доменные учетные записи для служб Сервера администрирования и сделать их членами глобальной доменной группы безопасности KLAdmins.
2. Задать в инсталляторе Сервера администрирования созданные доменные учетные (см. стр. 250) записи для служб.

## См. также:



## Задание папки общего доступа

Во время установки Сервера администрирования можно задать месторасположение папки общего доступа. Также месторасположение папки общего доступа можно задать после установки, в свойствах Сервера администрирования (см. стр. 707). По умолчанию папка общего доступа создается на устройстве с Сервером администрирования (с доступом на чтение для встроенной группы **Everyone**). Однако в некоторых случаях (таких как высокая нагрузка или необходимость доступа из изолированной сети) целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

Папка общего доступа используется в нескольких сценариях развертывания Агента администрирования.

Учет регистра для общей папки должен быть выключен.

См. также:



## Удаленная инсталляция средствами Сервера администрирования с помощью групповых политик Active Directory

В случае если устройства находятся в домене Windows (нет рабочих групп), первоначальное развертывание (установку Агента администрирования и программы безопасности на пока еще не управляемые устройства) целесообразно выполнять при помощи групповых политик Active Directory. Развертывание выполняется с помощью штатной задачи удаленной инсталляции Kaspersky Security Center. Если размер сети велик, с целью уменьшения нагрузки на дисковую подсистему устройства с Сервером администрирования целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

## Удаленная инсталляция рассылкой UNC-пути на автономный пакет

В случае если пользователи устройств сети организации имеют права локального администратора, еще одним способом первоначального развертывания является создание автономного пакета Агента администрирования (или даже "спаренного" пакета Агента администрирования совместно с программой безопасности). После создания автономного пакета нужно отправить пользователям устройств сети ссылку на пакет, находящийся в папке общего доступа. Инсталляция запускается по ссылке.

## Обновление из общей папки Сервера администрирования

В задаче обновления антивируса можно настроить обновление из папки общего доступа Сервера администрирования. Если задача назначена для большого количества устройств, целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

## Установка образов операционных систем

Установка образов операционных систем всегда выполняется с использованием папки общего доступа: устройства читают из папки образы операционных систем. Если планируется развертывание образов на большом количестве устройств организации, то целесообразно располагать папку общего доступа на специализированном файловом ресурсе.

См. также:

kaspersky

### Указание адреса Сервера администрирования

При установке Сервера администрирования можно задать адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования.

В качестве адреса Сервера администрирования вы можете указать:

- NetBIOS-имя Сервера администрирования, указанное по умолчанию.
- Полное доменное имя (FQDN) Сервера администрирования, если система доменных имен (DNS) в сети организации настроена и работает должным образом.
- Внешний адрес, если Сервер администрирования установлен в демилитаризованной зоне (DMZ).

В дальнейшем адрес Сервера администрирования можно будет изменить средствами Консоли администрирования, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

## Стандартная установка

Стандартная установка – это установка Сервера администрирования, при которой используются заданные по умолчанию пути для файлов программы, устанавливается набор плагинов по умолчанию и не включается Управление мобильными устройствами.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

### См. также:

Основной сценарий установки.....92

### В этом разделе

## Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка программы будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

## Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Стандартная**.

Стандартная установка рекомендуется, если вы хотите ознакомиться с программой Kaspersky Security Center, например, протестировать ее работу на небольшом участке сети вашей организации. При стандартной установке вы настраиваете только параметры базы данных. Параметры Сервера администрирования не настраиваются, для них используются заданные по умолчанию значения. Стандартная установка не позволяет выбрать устанавливаемые плагины управления, устанавливается заданный по умолчанию набор плагинов. Во время стандартной установки инсталляционные пакеты для мобильных устройств не создаются. Вы можете создать их позже в Консоли администрирования.

## Шаг 3. Установка Kaspersky Security Center 14.2 Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center 14.2 Web Console не работает с 32-разрядными операционными системами.

По умолчанию будут установлены и Kaspersky Security Center 14.2 Web Console, и Консоль администрирования на основе консоли Microsoft Management Console (MMC).

► *Если вы хотите установить только Kaspersky Security Center 14.2 Web Console:*

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе веб-интерфейса**.

Установка Kaspersky Security Center 14.2 Web Console (см. стр. 950) запускается автоматически после завершения установки Сервера администрирования.

► *Если вы хотите установить только Консоль администрирования на основе консоли Microsoft Management Console (MMC):*

1. Выберите **Установить только одну из консолей**.
2. В раскрывающемся списке выберите **Консоль на основе MMC**.

## Шаг 4. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

*Таблица 48. Зависимость параметров установки от выбора размеров сети*

| Параметры | 1 – 100 устройств | 101 – 1000 устройств | 1001 – 5000 устройств | Более 5000 устройств |
|---|---|---|---|---|
| Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Распределение времени запуска задачи обновления на клиентских устройствах случайным образом | Отсутствует | в интервале 5 минут | в интервале 10 минут | в интервале 10 минут |

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать программу для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

## Шаг 5. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или Microsoft SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip).

См. также:

Выбор СУБД ..... 164

## Шаг 6. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server (SQL Server Express)** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. стр. 234), укажите в поле **Имя экземпляра SQL Server** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя SQL Server**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией https://docs.microsoft.com/ru-RU/sql/database-engine/availability-groups/windows/availability-modes-

always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode, когда включена функция Always On.

- В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя установленного экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **Postgres** на предыдущем шаге:
  - В поле **Имя Postgres-сервера** укажите имя установленного экземпляра SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
  - В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

## Шаг 7. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Программа проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вы должны указать правильные учетные данные.

Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

### Шаг 8. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль администрирования на основе MMC.**
- **Запустить Kaspersky Security Center Web Console.**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center 14.2 Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Готово**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center 14.2 Web Console вы можете выполнить первоначальную настройку программы (см. стр. 285).

По окончании работы мастера установки следующие компоненты программы будут установлены на жесткий диск, на котором установлена операционная система:

- Сервер администрирования (совместно с серверной версией Агента администрирования);
- Консоль администрирования на основе консоли управления Microsoft Management Console (MMC);
- Kaspersky Security Center 14.2 Web Console (если выбрана ее установка);
- доступные в дистрибутиве плагины управления программами.

Кроме того, будет установлена программа Microsoft Windows Installer версии 4.5, если эта программа не была установлена ранее.

## Выборочная установка

Выборочная установка – это установка Сервера администрирования, при которой вам предлагается выбрать компоненты для установки и указать папку, в которую будет установлена программа.

С помощью этого типа установки вы можете настроить параметры базы данных, параметры Сервера администрирования, установить компоненты, которые не включены в стандартную установку и плагины управления защитными программами "Лаборатории Касперского". Вы можете также включить Управление мобильными устройствами.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на локальное устройство,*

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

## См. также:



## В этом разделе



## Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка программы будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

## Шаг 2. Выбор типа установки

В окне выбора типа установки укажите тип **Выборочная**.

Выборочная установка позволяет настроить параметры Kaspersky Security Center, такие как путь к папке общего доступа, учетные записи и порты подключения к Серверу администрирования, и параметры базы данных. Выборочная установка позволяет указать, какие плагины управления программами "Лаборатории Касперского" будут установлены. При выборочной установке вы можете создать инсталляционные пакеты для мобильных устройств, указав соответствующий параметр.

## Шаг 3. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования (см. стр. 809).
- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке программы на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки программы во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить нельзя.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

## Шаг 3. Установка Kaspersky Security Center 14.2 Web Console

Этот шаг отображается, только если вы используете 64-разрядную операционную систему. В противном случае этот шаг не отображается, поскольку Kaspersky Security Center 14.2 Web Console не работает с 32-разрядными операционными системами.

Если требуется установить Kaspersky Security Center 14.2 Web Console на то же устройство, что и Kaspersky Security Center, установите флажок **Установить Kaspersky Security Center 14.2 Web Console**. Если этот флажок не установлен, Kaspersky Security Center 14.2 Web Console не будет установлена. Будет установлена только Консоль администрирования на основе Microsoft Management Console (MMC). Однако если вы

используете 64-разрядную операционную систему, можно установить Kaspersky Security Center 14.2 Web Console позже, после начала работы с Kaspersky Security Center.

## Шаг 5. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

*Таблица 49. Зависимость параметров установки от выбора размеров сети*

| Параметры | 1 – 100 устройств | 101 – 1000 устройств | 1001 – 5000 устройств | Более 5000 устройств |
|---|---|---|---|---|
| Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Распределение времени запуска задачи обновления на клиентских устройствах случайным образом | Отсутствует | в интервале 5 минут | в интервале 10 минут | в интервале 10 минут |

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать программу для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

## Шаг 6. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или Microsoft SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip).

## Шаг 7. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server (SQL Server Express)** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. стр. 234), укажите в поле **Имя экземпляра SQL Server** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя SQL Server**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией https://docs.microsoft.com/ru-RU/sql/database-engine/availability-groups/windows/availability-modes-always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode, когда включена функция Always On.
  - В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

  Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.

- Если вы выбрали **MySQL** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя установленного экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.
  - В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.
- Если вы выбрали **Postgres** на предыдущем шаге:
  - В поле **Имя Postgres-сервера** укажите имя установленного экземпляра SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.
  - В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

См. также:

Основной сценарий установки.....92

## Шаг 8. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Программа проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вы должны указать правильные учетные данные.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

- Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

## Шаг 9. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Программа создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. стр. 250) и СУБД (см. стр. 246) на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. стр. 246), расположенный на другом устройстве, и / или если вы планируете разместить папку общего доступа (см. стр. 250) на другом устройстве.

  Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

  Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

  *Чтобы указать MSA или gMSA:*

  1. Нажмите на кнопку **Обзор**.
  2. В появившемся окне нажмите на кнопку **Тип объекта**.
  3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **OK**.
  4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. стр. 218).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch) (см. стр. 682).

### См. также:

Учетные записи для работы с СУБД ..... 218
Изменения в системе после установки Kaspersky Security Center ..... 277
Основной сценарий установки ..... 92

## Шаг 10. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. стр. 236).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

### См. также:

Изменения в системе после установки Kaspersky Security Center.....277

Основной сценарий установки.....92

## Шаг 11. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки программ (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки программных компонентов Kaspersky Security Center.

Вы можете определить общую папку (см. стр. 236) позже, если нужно.

## Шаг 12. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- **SSL-порт**

  Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования: 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию выбран вариант **2048 бит (большая безопасность)**.

Если Сервер администрирования работает под управлением Microsoft Windows XP с Service Pack 2, то встроенный сетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на устройстве, на котором установлен Сервер администрирования, эти порты нужно открыть вручную.

### См. также:

Порты, используемые Kaspersky Security Center ..... 98

Взаимодействие компонентов Kaspersky Security Center и программ безопасности: дополнительные сведения ..... 136

## Шаг 13. Задание адреса Сервера администрирования

Укажите адрес Сервера администрирования одним из следующих способов:

- **Имя DNS-домена**. Этот способ можно использовать в том случае, когда в сети присутствует DNS-сервер и клиентские устройства могут получить с его помощью адрес Сервера администрирования.

- **NetBIOS-имя**. Этот способ можно использовать либо если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, либо если в сети присутствует WINS-сервер.
- **IP-адрес**. Этот способ можно использовать, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

Если вы устанавливаете Kaspersky Security Center на активный узел отказоустойчивого кластера "Лаборатории Касперского" и создали виртуальный сетевой адаптер, во время подготовки узлов кластера (см. стр. 256) укажите IP-адрес этого адаптера. В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

## Шаг 14. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или систему доменных имен (DNS) Сервера администрирования.

## Шаг 15. Выбор плагинов управления программами

Выберите плагины управления программами "Лаборатории Касперского", которые требуется установить совместно с Kaspersky Security Center.

Для удобства поиска плагины разделены на группы в зависимости от типа защищаемых объектов.

## Шаг 16. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль администрирования на основе MMC.**
- **Запустить Kaspersky Security Center Web Console.**

  Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center 14.2 Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Готово**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center 14.2 Web Console вы можете выполнить первоначальную настройку программы (см. стр. 285).

kaspersky

# Развертывание отказоустойчивого кластера "Лаборатории Касперского"

Этот раздел содержит общую информацию об отказоустойчивом кластере "Лаборатории Касперского", а также инструкции по подготовке и развертыванию отказоустойчивого кластера "Лаборатории Касперского" в вашей сети.

## См. также:



## В этом разделе



## Сценарий: Развертывание отказоустойчивого кластера "Лаборатории Касперского"

Отказоустойчивый кластер "Лаборатории Касперского" обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

### Предварительные требования

У вас есть оборудование, соответствующее требованиям (см. стр. 254) для отказоустойчивого кластера.

### Этапы

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

a. **Создание учетной записи для служб Kaspersky Security Center**

   Создайте доменную группу (в этом сценарии для группы используется имя "KLAdmins") и предоставьте права локального администратора группе на обоих узлах и на файловом сервере. Затем создайте две учетные записи пользователей домена (в этом сценарии для этих учетных записей используются имена "ksc" и "rightless") и добавьте учетные записи в доменную группу KLAdmins.

   Добавьте учетную запись пользователя, под которой будет установлен Kaspersky Security Center, в ранее созданную доменную группу KLAdmins.

b. **Подготовка файлового сервера**

Подготовьте файловый сервер к работе в составе отказоустойчивого кластера "Лаборатории Касперского". Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям, создайте две общие папки для данных Kaspersky Security Center и настройте права доступа к общим папкам.

Инструкции: Подготовка файлового сервера для отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 255)

c. **Подготовка активного и пассивного узлов**

Подготовьте два компьютера с идентичным аппаратным и программным обеспечением для работы в качестве активного и пассивного узлов.

Инструкции: Подготовка узлов для отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 256)

d. **Установка системы управления базами данных (СУБД)**

Выберите любую из поддерживаемых СУБД (см. стр. 69) и установите СУБД на выделенный компьютер.

e. **Установка Kaspersky Security Center**

Установите Kaspersky Security Center в режиме отказоустойчивого кластера на оба узла. Сначала необходимо установить Kaspersky Security Center на активный узел, а затем установить его на пассивный.

Также вы можете установить Kaspersky Security Center 14.2 Web Console (см. стр. 960) на отдельном устройстве, не являющемся узлом кластера.

Инструкции: Установка Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 257)

f. **Тестирование отказоустойчивого кластера**

Убедитесь, что вы правильно настроили отказоустойчивый кластер и правильно ли он работает. Например, вы можете остановить одну из служб Kaspersky Security Center на активном узле: kladminserver, klnagent, ksnproxy, klactprx или klwebsrv. После остановки службы управление защитой должно быть автоматически переключено на пассивный узел.

**Результаты**

Отказоустойчивый кластер "Лаборатории Касперского" развернут. Пожалуйста, ознакомьтесь с событиями, которые приводят к переключению между активными и пассивными узлами (см. стр. 254).

## См. также:



## Об отказоустойчивом кластере "Лаборатории Касперского"

Отказоустойчивый кластер "Лаборатории Касперского" обеспечивает высокую доступность Kaspersky Security Center и минимизирует простои Сервера администрирования в случае сбоя. Отказоустойчивый кластер основан на двух идентичных экземплярах Kaspersky Security Center, установленных на двух компьютерах. Один из экземпляров работает как активный узел, а другой – как пассивный. Активный узел управляет защитой клиентских устройств, в то время как пассивный готов взять на себя все функции

активного узла в случае отказа активного узла. Когда происходит сбой, пассивный узел становится активным, а активный узел становится пассивным.

**Аппаратные и программные требования**

Для развертывания отказоустойчивого кластера "Лаборатории Касперского" у вас должно быть следующее оборудование:

- Два компьютера с одинаковым оборудованием и программным обеспечением. Эти компьютеры будут действовать как активный и пассивный узлы.
- Файловый сервер, поддерживающий протокол CIFS/SMB версии 2.0 или выше. Вы должны предоставить выделенный компьютер, который будет выступать в качестве файлового сервера.

  Убедитесь, что вы обеспечили высокую пропускную способность сети между файловым сервером, активным и пассивным узлами.

- Компьютер с системой управления базами данных (СУБД).

**Условия переключения**

Отказоустойчивый кластер переключает управление защитой клиентских устройств с активного узла на пассивный, если на активном узле происходит любое из следующих событий:

- Активный узел сломан из-за программного или аппаратного сбоя.
- Активный узел был временно остановлен для проведения технических работ (см. стр. 258).
- По крайней мере, одна из служб (или процессов) Kaspersky Security Center завершилась с ошибкой или была намеренно остановлена пользователем. К службам Kaspersky Security Center относятся: kladminserver, klnagent, klactprx и klwebsrv.
- Сетевое соединение между активным узлом и хранилищем на файловом сервере было прервано или разорвано.

## См. также:

Установка Сервера администрирования на отказоустойчивом кластере Microsoft .....260

Обновление Kaspersky Security Center на узлах отказоустойчивого кластера "Лаборатории Касперского" .....282

## Подготовка файлового сервера для отказоустойчивого кластера "Лаборатории Касперского"

Файловый сервер работает как обязательный компонент отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 254).

► *Чтобы подготовить файловый сервер:*

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям (см. стр. 254).
2. Убедитесь, что либо файловый сервер и оба узла (активный и пассивный) включены в один домен, либо файловый сервер является контроллером домена.

3. На файловом сервере создайте две общие папки. Один из них используется для хранения информации о состоянии отказоустойчивого кластера. Другая используется для хранения данных и параметров Kaspersky Security Center. Вам нужно будет указать пути к общим папкам при установке Kaspersky Security Center (см. стр. 257).
4. Предоставьте права полного доступа (как права общего доступа, так и NTFS-разрешения) к созданным общим папкам для следующих учетных записей пользователей и групп:
   - Доменная группа KLAdmins.
   - Учетные записи пользователей $<node1> и $<node2>. Здесь <node1> и <node2> – это имена компьютеров активного и пассивного узлов.

Файловый сервер подготовлен. Чтобы развернуть отказоустойчивый кластер "Лаборатории Касперского", следуйте инструкциям этого сценария (см. стр. 253).

## См. также:

Об отказоустойчивом кластере "Лаборатории Касперского".....254

Сценарий:Развертывание отказоустойчивого кластера "Лаборатории Касперского".....253

## Подготовка узлов для отказоустойчивого кластера "Лаборатории Касперского"

Подготовьте два компьютера к работе в качестве активного и пассивного узла для отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 254).

► *Чтобы подготовить узлы для отказоустойчивого кластера "Лаборатории Касперского":*

1. Убедитесь, что у вас есть два компьютера, соответствующих аппаратным и программным требованиям (см. стр. 254). Эти компьютеры будут действовать как активные и пассивные узлы отказоустойчивого кластера.
2. Убедитесь, что файловый сервер и оба узла включены в один домен.
3. Выполните одно из следующих действий:
   - На каждом из узлов создайте виртуальный сетевой адаптер. Вы можете сделать это с помощью программы стороннего производителя.

     Убедитесь, что выполняются следующие условия:
     - Виртуальные сетевые адаптеры должны быть отключены. Вы можете создать виртуальные сетевые адаптеры в отключенном состоянии или отключить их после создания.
     - Виртуальные сетевые адаптеры на обоих узлах должны иметь одинаковый IP-адрес.
   - Используйте сторонний балансировщик нагрузки. Например, вы можете использовать сервер nginx. В этом случае сделайте следующее:
     a. Предоставьте выделенный компьютер с операционной системой Linux с установленным nginx.
     b. Настройте балансировку нагрузки. Установите активный узел в качестве основного сервера и пассивный узел в качестве резервного сервера.
     c. На сервере nginx откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13291, TCP 13299 и TCP 17000.
4. Перезагрузите оба узла и файловый сервер.

5. Сопоставьте две общие папки, которые вы создали во время этапа подготовки файлового сервера (см. стр. 255), к каждому из узлов. Вы должны сопоставить общие папки как сетевые диски. При сопоставлении папок вы можете выбрать любые свободные буквы дисков. Для доступа к общим папкам используйте учетные данные учетной записи пользователя, которую вы создали на шаге 1 сценария (см. стр. 253).

Узлы подготовлены. Чтобы развернуть отказоустойчивый кластер "Лаборатории Касперского", следуйте инструкциям сценария (см. стр. 253).

## См. также:

Об отказоустойчивом кластере "Лаборатории Касперского".....254

Сценарий:Развертывание отказоустойчивого кластера "Лаборатории Касперского".....253

## Установка Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского"

Kaspersky Security Center устанавливается на оба узла отказоустойчивого кластера "Лаборатории Касперского" по отдельности. Сначала вы устанавливаете программу на активный узел, затем на пассивный. Во время установки вы выбираете, какой узел будет активным, а какой пассивным.

Только пользователь из доменной группы KLAdmins может установить Kaspersky Security Center на каждый узел.

► *Чтобы установить Kaspersky Security Center на активный узел отказоустойчивого кластера "Лаборатории Касперского":*

1. запустите исполняемый файл ksc_14.2.<номер сборки>_full_<язык>.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **положения и условия настоящего Лицензионного соглашения;**
   - **Политику конфиденциальности, которая описывает обработку данных.**

   Установка программы будет продолжена после установки обоих флажков.

   Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

3. Выберите **Первичный узел отказоустойчивого кластера "Лаборатории Касперского"**, чтобы установить программу на активный узел.

4. В окне **Общая папка** выполните следующее:

   - В полях **Общая папка состояний** и **Общая папка данных** укажите пути к общим папкам, которые вы создали на файловом сервере во время его подготовки (см. стр. 255).

- В полях **Общая папка состояний диска** и **Общая папка данных диска** выберите сетевые диски, к которым вы подключили общие папки во время подготовки узлов (см. стр. 256).
- Выберите режим подключения кластера: через виртуальный сетевой адаптер или сторонний балансировщик нагрузки.

5. Выполните другие шаги выборочной установки, начиная с шага 3 (см. стр. 245).

> На шаге 13 (см. стр. 251) укажите IP-адрес виртуального сетевого адаптера, если вы создали адаптер, во время подготовки узлов кластера (см. стр. 256). В противном случае введите IP-адрес стороннего балансировщика нагрузки, который вы используете.

Программа Kaspersky Security Center установлена на активном узле.

► *Чтобы установить Kaspersky Security Center на пассивный узел отказоустойчивого кластера "Лаборатории Касперского":*

1. запустите исполняемый файл ksc_14.2.<номер сборки>_full_<язык>.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

2. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

   - **положения и условия настоящего Лицензионного соглашения;**
   - **Политику конфиденциальности, которая описывает обработку данных.**

   Установка программы будет продолжена после установки обоих флажков.

   Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

3. Выберите **Вторичный узел отказоустойчивого кластера "Лаборатории Касперского"**, чтобы установить программу на пассивный узел.
4. В окне **Общая папка** в поле **Общая папка состояний** укажите путь к общей папке с информацией о состоянии кластера, который вы создали на файловом сервере во время его подготовки (см. стр. 255).
5. Нажмите на кнопку **Установить**. После завершения установки нажмите на кнопку **Готово**.

Программа Kaspersky Security Center установлена на пассивный узел. Теперь вы можете протестировать отказоустойчивый кластер "Лаборатории Касперского", чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

### См. также:

Обновление Kaspersky Security Center на узлах отказоустойчивого кластера "Лаборатории Касперского" ..... 282

## Запуск и остановка узла кластера вручную

Вам может потребоваться остановить весь отказоустойчивый кластер "Лаборатории Касперского" или временно отключить один из узлов кластера для обслуживания. В этом случае следуйте инструкциям этого

раздела. Не пытайтесь запускать или останавливать службы или процессы, связанные с отказоустойчивым кластером, с помощью других средств. Это может привести к потере данных.

**Запуск и остановка всего отказоустойчивого кластера для обслуживания**

► *Чтобы запустить или остановить весь отказоустойчивый кластер:*

1. На активном узле перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Откройте командную строку и выполните одну из следующих команд:
   - Чтобы остановить кластер, выполните: `klfoc -stopcluster --stp klfoc`
   - Чтобы запустить кластер, выполните: `klfoc -startcluster --stp klfoc`

   Отказоустойчивый кластер запускается или останавливается в зависимости от команды.

**Обслуживание одного из узлов**

► *Для обслуживания одного из узлов:*

1. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
2. На узле, который вы хотите обслуживать, перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Откройте командную строку и отключите узел от кластера, выполнив команду `detach_node.cmd`.
4. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.
5. Выполните работы по техническому обслуживанию.
6. На активном узле остановите отказоустойчивый кластер с помощью команды `klfoc -stopcluster --stp klfoc`.
7. На обслуживаемом узле перейдите в папку <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Откройте командную строку и подключите узел к кластеру, выполнив команду `attach_node.cmd`.
9. На активном узле запустите отказоустойчивый кластер с помощью команды `klfoc -startcluster --stp klfoc`.

Узел обслуживается и подключается к отказоустойчивому кластеру.

## См. также:

Об отказоустойчивом кластере "Лаборатории Касперского".....254

Сценарий:Развертывание отказоустойчивого кластера "Лаборатории Касперского".....253

kaspersky

# Установка Сервера администрирования на отказоустойчивом кластере Microsoft

Процедура установки Сервера администрирования на отказоустойчивом кластере отличается как от стандартной, так и от выборочной установки на автономном устройстве.

Выполните процедуру, описанную в этом разделе, на узле, который содержит общее хранилище данных кластера.

► *Чтобы установить Сервер администрирования Kaspersky Security Center на кластер,*

запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации>.exe.

Откроется окно с выбором программ "Лаборатории Касперского" для установки. В окне с выбором программ по ссылке **Установить Сервер администрирования Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.

## В этом разделе



## Шаг 1. Просмотр Лицензионного соглашения и Политики конфиденциальности

На этом шаге мастера установки требуется ознакомиться с Лицензионным соглашением, которое заключается между вами и "Лабораторией Касперского", и Политикой конфиденциальности.

Вам также может быть предложено ознакомиться с Лицензионными соглашениями и Политиками конфиденциальности на доступные в дистрибутиве Kaspersky Security Center плагины управления программами.

Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности, подтвердите это, установив соответствующие флажки.

Установка программы будет продолжена после установки обоих флажков.

Если вы не согласны с Лицензионным соглашением или Политикой конфиденциальности, то отмените установку программы, нажав на кнопку **Отмена**.

## Шаг 2. Выбор типа установки на кластер

Выберите тип установки на кластере:

- **Кластер (установить на всех узлах кластера)**

  Рекомендуется выбрать этот параметр. Если вы выберете этот параметр, Сервер администрирования будет установлен на всех узлах кластера одновременно.

  > На шаге выбора Консоли администрирования для установки (см. стр. 239) требуется выбрать Консоль, которая будет установлена на текущем узле кластера. Если вы устанавливаете Консоль только на узле кластера, в случае сбоя узла вы потеряете доступ к Серверу администрирования. Рекомендуется на этом шаге (см. стр. 239) выбрать Консоль администрирования на основе консоли Microsoft Management Console (MMC) для установки на все узлы кластера. После установки Сервера администрирования установите Kaspersky Security Center 14.2 Web Console (см. стр. 960) на отдельном устройстве, не являющемся узлом кластера. Это позволяет управлять Сервером администрирования с помощью Kaspersky Security Center 14.2 Web Console в случае сбоя узла кластера.

- **Локально (установить только на это устройство)**

  Если вы выберете этот параметр, Сервер администрирования будет установлен только на текущем узле, как на автономном сервере, и Сервер администрирования не будет работать как кластерная программа. Например, вы можете выбрать этот параметр для экономии свободного пространства в общем хранилище, если отказоустойчивость не требуется для Сервера администрирования. В случае выхода из строя текущего узла вам придется установить Сервер администрирования на другой узел и восстановить состояние Сервера администрирования из резервной копии данных.

Дальнейшие действия такие же, как при использовании стандартного (см. стр. 238) или выборочного (см. стр. 243) способа установки, начиная с шага выбора способа установки.

## Шаг 3. Указание имени виртуального Сервера администрирования

Укажите сетевое имя нового виртуального Сервера администрирования. Вы сможете использовать это имя для подключения Консоли администрирования или Kaspersky Security Center 14.2 Web Console к Серверу администрирования.

Указанное имя должно отличаться от имени кластера.

## Шаг 4. Указание параметров сети виртуального Сервера администрирования

► *Чтобы указать сетевые данные нового экземпляра виртуального Сервера администрирования:*

1. В разделе **Сеть для использования** выберите сеть домена, к которой подключен текущий узел кластера.
2. Выполните одно из следующих действий:
   - Если DHCP используется в выбранной сети для назначения IP-адресов, выберите параметр **Использовать DHCP**.
   - Если DHCP не используется в выбранной сети, укажите требуемый IP-адрес.

     Указанный вами IP-адрес должен отличаться от IP-адреса кластера.
3. Нажмите на кнопку **Добавить**, чтобы применить указанные параметры.

Вы сможете использовать автоматически назначенный или указанный IP-адрес для подключения Консоли администрирования или Kaspersky Security Center Web Console к Серверу администрирования.

## Шаг 5. Указание группы кластеров

Группа кластера – это особая роль отказоустойчивого кластера, которая содержит общие ресурсы для всех узлов. У вас есть два варианта:

- Создание новой кластерной группы.

  Этот вариант рекомендуется в большинстве случаев. Новая группа кластера будет содержать все общие ресурсы, относящиеся к экземпляру Сервера администрирования.
- Выбор существующей группы кластеров.

  Выберите этот параметр, если вы хотите использовать общий ресурс, который уже связан с существующей группой кластера. Например, вы можете использовать этот вариант, если хотите использовать хранилище, связанное с существующей группой кластера, и если нет другого доступного хранилища для новой группы кластера.

## Шаг 6. Выбор кластерного хранилища данных

► *Чтобы выбрать кластерное хранилище данных:*

1. В разделе **Доступные хранилища** выберите хранилище, в которое будут установлены общие ресурсы экземпляра виртуального Сервера администрирования.
2. Если выбранное хранилище данных содержит несколько томов, в разделе **Доступные разделы на диске** выберите нужный том.
3. В поле **Путь установки** введите путь к общему хранилищу данных, в который будут установлены ресурсы экземпляра виртуального Сервера администрирования.

Хранилище данных выбрано.

## Шаг 7. Указание учетной записи для удаленной установки

Укажите имя пользователя и пароль, которые будут использоваться для удаленной установки экземпляра виртуального Сервера администрирования на пассивный узел кластера.

Для указанной вами учетной записи должны быть предоставлены права администратора на всех узлах кластера.

## Шаг 8. Выбор компонентов для установки

Выберите компоненты Сервера администрирования Kaspersky Security Center, которые вы хотите установить:

- **Управление мобильными устройствами**. Установите этот флажок, если требуется создать инсталляционные пакеты для мобильных устройств во время работы мастера установки Kaspersky Security Center. Вы можете также создать инсталляционные пакеты для мобильных устройств вручную, после установки Сервера администрирования средствами Консоли администрирования (см. стр. 809).
- **Агент SNMP**. Получает статистическую информацию для Сервера администрирования по протоколу SNMP. Компонент доступен при установке программы на устройство с установленным компонентом SNMP.

  После установки Kaspersky Security Center необходимые для получения статистической информации mib-файлы будут расположены в папке установки программы во вложенной папке SNMP.

Компоненты Агент администрирования и Консоль администрирования не отображаются в списке компонентов. Эти компоненты устанавливаются автоматически, их установку отменить нельзя.

На этом шаге мастера также следует указать папку для установки компонентов Сервера администрирования. По умолчанию компоненты устанавливаются в папку <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Если папки с таким названием нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.

## Шаг 9. Выбор размера сети

Укажите размер сети, в которой устанавливается Kaspersky Security Center. В зависимости от количества устройств в сети мастер настраивает параметры установки и отображение интерфейса программы.

В таблице ниже перечислены параметры установки программы и отображения интерфейса при выборе разных размеров сети.

*Таблица 50. Зависимость параметров установки от выбора размеров сети*

| Параметры | 1 – 100 устройств | 101 – 1000 устройств | 1001 – 5000 устройств | Более 5000 устройств |
|---|---|---|---|---|
| Отображение в дереве консоли узла подчиненных и виртуальных Серверов администрирования и всех параметров, связанных с подчиненными и виртуальными Серверами | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Отображение разделов **Безопасность** в окнах свойств Сервера и групп администрирования | Отсутствует | Отсутствует | Присутствует | Присутствует |
| Распределение времени запуска задачи обновления на клиентских устройствах случайным образом | Отсутствует | в интервале 5 минут | в интервале 10 минут | в интервале 10 минут |

При подключении Сервера администрирования к серверу базы данных MySQL 5.7 и SQL Express не рекомендуется использовать программу для управления более чем 10 000 устройств. Для системы управления базами данных MariaDB максимальное рекомендуемое количество управляемых устройств составляет 20 000.

## Шаг 10. Выбор базы данных

На этом шаге мастера выберите одну из следующих систем управления базами данных (СУБД), которая будет использоваться для хранения базы данных Сервера администрирования:

- **Microsoft SQL Server или Microsoft SQL Server Express**
- **MySQL или MariaDB**
- **PostgreSQL или Postgres Pro**

Рекомендуется устанавливать Сервер администрирования на выделенный сервер, а не на контроллер домена. Если вы устанавливаете Kaspersky Security Center на сервер, выполняющий роль контроллера домена только для чтения (RODC), Microsoft SQL Server (SQL Express) не должен быть установлен локально (на этом же устройстве). В этом случае рекомендуется установить Microsoft SQL Server (SQL Express) удаленно (на другое устройство) или использовать MySQL, MariaDB или PostgreSQL, если вам нужно установить СУБД локально.

Структура базы данных Сервера администрирования представлена в файле klakdb.chm, который находится в папке установки Kaspersky Security Center. Этот файл также доступен в архиве на портале "Лаборатории Касперского": klakdb.zip (https://media.kaspersky.com/utilities/CorporateUtilities/klakdb.zip).

## Шаг 11. Настройка параметров SQL-сервера

На этом шаге мастера укажите следующие параметры подключения в зависимости от выбранной вами системы управления базами данных (СУБД):

- Если вы выбрали **Microsoft SQL Server (SQL Server Express)** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя SQL-сервера, установленного в сети. При помощи кнопки **Обзор** вы можете открыть список всех SQL-серверов, установленных в сети. По умолчанию поле не заполнено.

    Если вы подключаетесь к SQL Server через пользовательский порт, то вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_host_name,1433
    ```

    Если вы защищаете соединение между Сервером администрирования и SQL Server с помощью сертификата (см. стр. 234), укажите в поле **Имя экземпляра SQL Server** то же имя экземпляра, которое использовалось при создании сертификата. Если вы используете именованный экземпляр SQL Server, вместе с именем экземпляра SQL Server укажите через запятую номер порта, например:

    ```
    SQL_Server_name,1433
    ```

    Если вы используете несколько экземпляров SQL Server на одном устройстве, дополнительно укажите через обратную косую черту имя экземпляра, например:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Если для SQL Server в корпоративной сети включена функция Always On, укажите имя прослушивателя группы доступности в поле **Имя SQL Server**. Обратите внимание, что Сервер администрирования поддерживает только режим доступности с синхронной фиксацией https://docs.microsoft.com/ru-RU/sql/database-engine/availability-groups/windows/availability-modes-always-on-availability-groups?view=sql-server-2016#SyncCommitAvMode, когда включена функция Always On.
  - В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

  Если на этом шаге вы хотите установить SQL-сервер на то устройство, с которого производите установку Kaspersky Security Center, нужно прервать установку и запустить ее снова после установки SQL-сервера. Поддерживаемые SQL-серверы перечислены в требованиях к системе.

  Если вы хотите установить SQL-сервер на удаленное устройство, прерывать работу мастера установки Kaspersky Security Center не требуется. Установите SQL Server и вернитесь к установке Kaspersky Security Center.
- Если вы выбрали **MySQL** на предыдущем шаге:
  - В поле **Имя SQL-сервера** укажите имя установленного экземпляра СУБД. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к базе данных DBMS-сервера. По умолчанию установлен порт 3306.

- В поле **Имя базы данных** задайте имя базы данных, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

- Если вы выбрали **Postgres** на предыдущем шаге:
  - В поле **Имя Postgres-сервера** укажите имя установленного экземпляра SQL-сервера. По умолчанию используется IP-адрес устройства, на который устанавливается Kaspersky Security Center.
  - В поле **Порт** укажите порт для подключения Сервера администрирования к СУБД. По умолчанию установлен порт 5432.

В поле **Имя базы данных** задайте имя СУБД, которая была создана для размещения информации Сервера администрирования. По умолчанию указано значение *KAV*.

## Шаг 12. Выбор режима аутентификации

Определите режим аутентификации, который будет использоваться при подключении Сервера администрирования к системе управления базами данных (СУБД).

В зависимости от выбранной СУБД вы можете выбрать следующие режимы аутентификации:

- Для SQL Express или Microsoft SQL Server выберите один из следующих вариантов:
  - **Режим аутентификации Microsoft Windows**. В этом случае при проверке прав будет использоваться учетная запись для запуска Сервера администрирования.
  - **Режим аутентификации SQL-сервера**. В случае выбора этого варианта для проверки прав будет использоваться указанная в окне учетная запись. Заполните поля **Учетная запись** и **Пароль**.

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

  Программа проверяет, доступна ли база данных для обоих режимов аутентификации. Если база данных недоступна, отображается сообщение об ошибке и вы должны указать правильные учетные данные.

  Если база данных Сервера администрирования находится на другом устройстве и учетная запись Сервера администрирования не имеет доступа к серверу базы данных, то при установке или обновлении Сервера администрирования следует использовать режим аутентификации SQL-сервера. Это может происходить в случае, когда устройство с базой данных находится не в домене, или Сервер администрирования установлен под учетной записью LocalSystem.

Для MySQL, MariaDB, PostgreSQL или Postgres Pro укажите учетную запись и пароль.

## Шаг 13. Выбор учетной записи для запуска Сервера администрирования

Выберите учетную запись, под которой Сервер администрирования будет запускаться как служба.

- **Создать учетную запись автоматически**. Программа создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования kladminserver.

  Вы можете выбрать этот вариант, если вы планируете разместить папку общего доступа (см. стр. 250) и СУБД (см. стр. 246) на том же устройстве, что и Сервер администрирования.

- **Выбрать учетную запись**. Служба Сервера администрирования (kladminserver) будет запускаться под выбранной вами учетной записью.

Вам потребуется выбрать доменную учетную запись, например, если вы планируете использовать в качестве СУБД SQL-сервер любого выпуска, в том числе SQL-express (см. стр. 246), расположенный на другом устройстве, и / или если вы планируете разместить папку общего доступа (см. стр. 250) на другом устройстве.

Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

Прежде чем выбрать MSA или gMSA, необходимо установить учетную запись на том же устройстве, на котором вы хотите установить Сервер администрирования. Если учетная запись еще не установлена, отмените установку Сервера администрирования, установите учетную запись и перезапустите установку Сервера администрирования. Подробнее об установке управляемых учетных записей служб на локальном устройстве см. в официальной документации Microsoft.

*Чтобы указать MSA или gMSA:*

1. Нажмите на кнопку **Обзор**.
2. В появившемся окне нажмите на кнопку **Тип объекта**.
3. Выберите тип **Учетная запись для служб** и нажмите на кнопку **OK**.
4. Выберите нужную учетную запись и нажмите на кнопку **OK**.

Выбранная вами учетная запись должна обладать различными правами в зависимости от того, какую СУБД вы планируете использовать (см. стр. 218).

Из соображений безопасности не делайте учетную запись, под которой запускается Сервер администрирования, привилегированной.

Если в дальнейшем вы захотите изменить учетную запись Сервера администрирования, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования (klsrvswch) (см. стр. 682).

## Шаг 14. Выбор учетной записи для запуска служб Kaspersky Security Center

Выберите учетную запись, под которой будут запускаться службы Kaspersky Security Center на этом устройстве:

- **Создать учетную запись автоматически**. Kaspersky Security Center создает локальную учетную запись KlScSvc на этом устройстве в группе kladmins. Службы Kaspersky Security Center будут запускаться под созданной учетной записью.
- **Выбрать учетную запись**. Службы Kaspersky Security Center будут запускаться под выбранной вами учетной записью.

  Вам потребуется выбрать доменную учетную запись, например, если вы планируете сохранять отчеты в папке, расположенной на другом устройстве, или же если этого требует политика безопасности в вашей организации. Также вам может потребоваться выбрать доменную учетную запись при установке Сервера администрирования на отказоустойчивый кластер (см. стр. 236).

Из соображений безопасности не делайте учетную запись, под которой запускаются службы, привилегированной.

Под выбранной учетной записью будут запускаться службы прокси-сервера KSN (ksnproxy), прокси-сервера активации "Лаборатории Касперского" (klactprx) и портала авторизации "Лаборатории Касперского" (klwebsrv).

## Шаг 15. Определение папки общего доступа

Определите место размещения и название папки общего доступа, которая будет использоваться для следующих целей:

- хранения файлов, необходимых для удаленной установки программ (файлы копируются на Сервер администрирования при создании инсталляционных пакетов);
- размещения обновлений, копируемых с источника обновлений на Сервер администрирования.

К этому ресурсу будет открыт общий доступ на чтение для всех пользователей.

Вы можете выбрать один из двух вариантов:

- **Создать папку общего доступа**. Создание новой папки. Укажите путь к папке в расположенном ниже поле.
- **Выбрать существующую папку общего доступа**. Выбор папки общего доступа из числа уже существующих.

Папка общего доступа может размещаться как локально на устройстве, с которого производится установка, так и удаленно, на любом из клиентских устройств, входящих в состав сети организации. Вы можете указать папку общего доступа с помощью кнопки **Обзор** или вручную, введя в соответствующем поле UNC-путь (например, \\server\Share).

По умолчанию создается локальная папка Share в папке, заданной для установки программных компонентов Kaspersky Security Center.

Вы можете определить общую папку (см. стр. 236) позже, если нужно.

## Шаг 16. Настройка параметров подключения к Серверу администрирования

Настройте параметры подключения к Серверу администрирования:

- **Порт**

  Номер порта, по которому выполняется подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- **SSL-порт**

  Номер SSL-порта, по которому осуществляется защищенное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- **Длина ключа шифрования**

Выберите длину ключа шифрования: 1024 бита или 2048 бит.

Ключ шифрования длиной 1024 бита оказывает меньшую нагрузку на процессор, но считается устаревшим и по техническим характеристикам может не обеспечивать надежное шифрование. Также есть вероятность, что имеющееся оборудование несовместимо с SSL-сертификатами с длиной ключа 1024 бита.

Ключ шифрования длиной 2048 бит отвечает современным стандартам шифрования. Однако использование 2048-битного ключа шифрования может привести к дополнительной нагрузке на процессор.

По умолчанию выбран вариант **2048 бит (большая безопасность)**.

Если Сервер администрирования работает под управлением Microsoft Windows XP с Service Pack 2, то встроенный сетевой экран блокирует TCP-порты с номерами 13000 и 14000. Поэтому для обеспечения доступа на устройстве, на котором установлен Сервер администрирования, эти порты нужно открыть вручную.

## Шаг 17. Задание адреса Сервера администрирования

Задайте адрес Сервера администрирования. Вы можете выбрать один из следующих вариантов:

- **Имя DNS-домена**. Этот способ можно использовать в том случае, когда в сети присутствует DNS-сервер и клиентские устройства могут получить с его помощью адрес Сервера администрирования.
- **NetBIOS-имя**. Этот способ можно использовать либо если клиентские устройства получают адрес Сервера администрирования с помощью протокола NetBIOS, либо если в сети присутствует WINS-сервер.
- **IP-адрес**. Этот способ можно использовать, если Сервер администрирования имеет статический IP-адрес, который в дальнейшем не будет изменяться.

## Шаг 18. Адрес Сервера для подключения мобильных устройств

Этот шаг мастера установки доступен, если вы выбрали для установки компонент Управление мобильными устройствами.

В окне **Адрес для подключения мобильных устройств** укажите внешний адрес Сервера администрирования для подключения мобильных устройств, которые находятся за пределами локальной сети. Вы можете указать IP-адрес или систему доменных имен (DNS) Сервера администрирования.

## Шаг 19. Распаковка и установка файлов на жесткий диск

По окончании настройки параметров установки компонентов Kaspersky Security Center вы можете запустить установку файлов на жесткий диск.

Если для запуска установки требуются дополнительные программы, мастер установки сообщит об этом перед началом установки Kaspersky Security Center в окне **Установка обязательных компонентов**. Необходимые программы будут установлены автоматически после нажатия на кнопку **Далее**.

На последней странице можно выбрать, какую консоль требуется запустить для работы с Kaspersky Security Center:

- **Запустить Консоль администрирования на основе MMC.**
- **Запустить Kaspersky Security Center Web Console.**

Этот параметр доступен, только если на одном из предыдущих шагов вы выбрали установку Kaspersky Security Center 14.2 Web Console.

Вы можете завершить работу мастера без запуска Kaspersky Security Center. Для этого нажмите на кнопку **Готово**. Работу с Kaspersky Security Center можно начать позже в любое время.

При первом запуске Консоли администрирования или Kaspersky Security Center 14.2 Web Console вы можете выполнить первоначальную настройку программы (см. стр. 285).

## Установка Сервера администрирования в неинтерактивном режиме

Сервер администрирования может быть установлен в неинтерактивном режиме, то есть без интерактивного ввода параметров установки.

► *Чтобы установить Сервер администрирования на локальном устройстве в неинтерактивном режиме:*

1. Прочитайте Лицензионное соглашение (см. стр. 343). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. Прочитайте Политику конфиденциальности (см. стр. 216). Используйте команду ниже, только если вы понимаете и соглашаетесь с тем, что мои данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.
3. выполните команду

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
```

где `setup_parameters` – список параметров и их значений, отделенных друг от друга пробелом (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Файл setup.exe расположен в папке Server внутри дистрибутива Kaspersky Security Center.

Имена и возможные значения параметров, которые можно использовать при установке Сервера администрирования в неинтерактивном режиме, приведены в таблице ниже.

*Таблица 51. Параметры установки Сервера администрирования в неинтерактивном режиме*

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| EULA | Согласие с условиями Лицензионного соглашения. | • 1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения.<br>• Другое значение или не задано – не согласны с условиями Лицензионного соглашения (установка не выполняется). |

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| PRIVACYPOLICY | Согласие с условиями Политики конфиденциальности. | • 1 – Я понимаю и соглашаюсь, что мои данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Я подтверждаю, что полностью прочитал(а) и понимаю Политику конфиденциальности.<br>• Другое значение или не задано – Я не принимаю условия Политики конфиденциальности (установка не выполняется). |
| INSTALLATIONMODETYPE | Тип установки Сервера администрирования. | • Standard – стандартная установка.<br>• Custom – выборочная установка. |
| INSTALLDIR | Путь к папке установки Сервера администрирования. | Строковое значение. |
| ADDLOCAL | Список компонентов (через запятую) Сервера администрирования для установки. | CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.<br>Минимальный достаточный для корректной установки Сервера администрирования список компонентов:<br>`ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.` |
| NETRANGETYPE | Размер сети (количество устройств в сети). | • NRT_1_100 – от 100 до 100 устройств.<br>• NRT_100_1000 – от 101 до 1000 устройств.<br>• NRT_GREATER_1000 – более 1000 устройств. |

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| SRV_ACCOUNT_TYPE | Способ задания учетной записи, под которой Сервер администрирования будет запускаться как служба. | • SrvAccountDefault – учетная запись создается автоматически.<br>• SrvAccountUser – учетная запись пользователя задана вручную. В этом случае требуется задать значения параметров SERVERACCOUNTNAME и SERVERACCOUNTPWD. |
| SERVERACCOUNTNAME | Имя учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser. | Строковое значение. |
| SERVERACCOUNTPWD | Пароль учетной записи, под которой Сервер администрирования будет запускаться как служба. Требуется задать значение параметра, если SRV_ACCOUNT_TYPE=SrvAccountUser. | Строковое значение. |
| SERVERCER | Длина ключа для сертификата Сервера администрирования (в битах). | • 1 – длина ключа для сертификата Сервера администрирования составляет 2048 бит.<br>• Значение не задано – длина ключа для сертификата Сервера администрирования составляет 1024 бит. |

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| DBTYPE | Тип базы данных, которая будет использоваться для размещения информационной базы данных Сервера администрирования.<br>Этот параметр является обязательным. | • MySQL – будет использоваться база данных MySQL или MariaDB. В этом случае следует задать значения параметров `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` и `MYSQLACCOUNTPWD`.<br>• MSSQL – будет использоваться база данных Microsoft SQL Server (SQL Express). В этом случае следует задать значения параметров `MSSQLSERVERNAME`, `MSSQLDBNAME`, `MSSQLAUTHTYPE`.<br>• POSTGRES – будет использоваться база данных PostgreSQL или Postgres Pro. В этом случае следует задать значения параметров `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` и `POSTGRESACCOUNTPWD`. |
| MYSQLSERVERNAME | Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MySQL. | Строковое значение. |
| MYSQLSERVERPORT | Номер порта для подключения к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MySQL. | Числовое значение. |
| MYSQLDBNAME | Имя базы данных, которая будет создана для размещения данных Сервера администрирования. Требуется задать значение параметра, если DBTYPE=MySQL. | Строковое значение. |
| MYSQLACCOUNTNAME | Имя учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL. | Строковое значение. |

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| MYSQLACCOUNTPWD | Пароль учетной записи для подключения к базе. Требуется задать значение параметра, если DBTYPE=MySQL. | Строковое значение. |
| MSSQLSERVERNAME | Полное имя SQL Server. Требуется задать значение параметра, если DBTYPE=MSSQL. | Строковое значение. |
| MSSQLDBNAME | Имя базы данных. Требуется задать значение параметра, если DBTYPE=MSSQL. | Строковое значение. |
| MSSQLAUTHTYPE | Тип авторизации при подключении к SQL-серверу. Требуется задать значение параметра, если DBTYPE=MSSQL. | • Windows – режим аутентификации Microsoft Windows.<br>• SQLServer – режим аутентификации SQL-сервера. В этом случае требуется задать значения параметров `MSSQLACCOUNTNAME` и `MSSQLACCOUNTPWD`. |
| MSSQLACCOUNTNAME | Имя учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer. | Строковое значение. |
| MSSQLACCOUNTPWD | Пароль учетной записи для подключения к SQL-серверу. Требуется задать значение параметра, если MSSQLAUTHTYPE=SQLServer. | Строковое значение. |
| CREATE_SHARE_TYPE | Способ задания папки общего доступа. | • Create – создать новую папку общего доступа. В этом случае требуется задать значения параметров `SHARELOCALPATH` и `SHAREFOLDERNAME`.<br>• ChooseExisting – выбрать существующую папку. В этом случае требуется задать значение параметра `EXISTSHAREFOLDERNAME`. |
| SHARELOCALPATH | Путь к локальной папке. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create | Строковое значение. |

| Имя параметра | Описание параметра | Доступные значения |
|---|---|---|
| SHAREFOLDERNAME | Сетевое имя папки общего доступа. Требуется задать значение параметра, если CREATE_SHARE_TYPE=Create. | Строковое значение. |
| EXISTSHAREFOLDERNAME | Полный путь к существующей папке общего доступа.<br>Требуется задать значение параметра, если CREATE_SHARE_TYPE=ChooseExisting. | Строковое значение. |
| SERVERPORT | Номер порта для подключения к Серверу администрирования. | Числовое значение. |
| SERVERSSLPORT | Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL | Числовое значение. |
| SERVERADDRESS | Адрес Сервера администрирования. | Строковое значение. |
| MOBILESERVERADDRESS | Адрес Сервера для подключения мобильных устройств. | Строковое значение. |

Подробно параметры установки Сервера администрирования описаны в разделе Выборочная установка (см. стр. 243).

### См. также:

Основной сценарий установки.....92

## Установка Консоли администрирования на рабочее место администратора

Вы можете установить Консоль администрирования отдельно на рабочее место администратора и управлять Сервером администрирования по сети с помощью этой Консоли.

► *Чтобы установить Консоль администрирования на рабочее место администратора:*

1. Запустите исполняемый файл setup.exe.

   Откроется окно с выбором программ "Лаборатории Касперского" для установки.

2. В окне с выбором программ по ссылке **Установить только Консоль администрирования Kaspersky Security Center** запустите мастер установки Консоли администрирования. Следуйте далее указаниям мастера.

3. Выберите папку назначения. По умолчанию это <Диск>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Если такой папки нет, она будет создана автоматически в процессе установки. Вы можете изменить папку назначения с помощью кнопки **Обзор**.
4. В завершающем окне мастера установки нажмите на кнопку **Запустить**, чтобы начать процесс установки Консоли администрирования.

По окончании работы мастера Консоль администрирования будет установлена на рабочем месте администратора.

► *Чтобы установить Консоль администрирования на рабочее место администратора в неинтерактивном режиме:*

1. Прочитайте Лицензионное соглашение (см. стр. 343). Используйте команду ниже, только если вы поняли и принимаете условия Лицензионного соглашения.
2. В папке `Distrib\Console` дистрибутива Kaspersky Security Center запустите файл setup.exe с помощью следующей команды:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Если вы хотите установить все плагины управления из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, выполните следующую команду:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Если вы хотите указать, какие плагины управления устанавливать из папки `Distrib\Console\Plugins` вместе с Консолью администрирования, укажите плагины управления после ключа "/p" и разделите их точкой с запятой:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   Здесь `P1`, `P2`, `P3` – имена плагинов управления, которые соответствуют именам папок плагинов управления в папке `Distrib\Console\Plugins`. Например:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

Консоль администрирования и плагины управления (если они были указаны) будут установлены на рабочее место администратора.

После установки Консоли администрирования следует подключиться к Серверу администрирования. Для этого нужно запустить Консоль администрирования и в открывшемся окне указать имя устройства или IP-адрес устройства, на котором установлен Сервер администрирования, а также параметры учетной записи для подключения к нему. После установления соединения с Сервером администрирования можно управлять системой антивирусной защиты с помощью этой Консоли администрирования.

Вы можете удалить Консоль администрирования стандартными средствами установки и удаления программ Microsoft Windows.

## См. также:

Основной сценарий установки.....92

# Изменения в системе после установки Kaspersky Security Center

### Значок Консоли администрирования

В результате установки Консоли администрирования на вашем устройстве появится значок для запуска Консоли администрирования. Вы можете найти Консоль администрирования в меню **Пуск** → **Программы** → **Kaspersky Security Center**.

### Службы Сервера администрирования и Агента администрирования

Сервер администрирования и Агент администрирования будут установлены на устройстве в качестве служб со свойствами, указанными в таблице ниже. В таблице также указаны атрибуты других служб, которые выполняются на устройстве после установки Сервера администрирования.

*Таблица 52. Свойства служб Kaspersky Security Center*

| Компонент | Имя службы | Отображаемое имя службы | Учетная запись |
|---|---|---|---|
| Сервер администрирования | kladminserver | Сервер администрирования Kaspersky Security Center | Указанная пользователем или специальная, созданная при установке, непривилегированная учетная запись вида KL-AK-* |
| Агент администрирования | klnagent | Агент администрирования Kaspersky Security Center | Локальная система |
| Веб-сервер для работы Kaspersky Security Center 14.2 Web Console и организации внутреннего портала организации | klwebsrv | Веб-сервер "Лаборатории Касперского" | Специальная непривилегированная учетная запись KlScSvc |
| Прокси-сервер активации | klactprx | Прокси-сервер активации "Лаборатории Касперского" | Специальная непривилегированная учетная запись KlScSvc |
| Прокси-сервер KSN | ksnproxy | Прокси-сервер Kaspersky Security Network | Специальная непривилегированная учетная запись KlScSvc |

### Службы Kaspersky Security Center 14.2 Web Console

Если вы установите Kaspersky Security Center 14.2 Web Console на устройство, то на нем будут выполняться следующие службы (см. таблицу ниже):

*Таблица 53. Службы Kaspersky Security Center 14.2 Web Console*

| Отображаемое имя службы | Учетная запись |
|---|---|
| Служба Kaspersky Security Center Web Console | NT Service/KSCSvcWebConsole |
| Kaspersky Security Center Web Console | Сетевая служба |
| Плагины Сервера администрирования Kaspersky Security Center | NT Service/KSCWebConsolePlugin |
| Служба управления Kaspersky Security Center Web Console | Локальная система |
| Очередь сообщений Kaspersky Security Center Web Console | NT Service/KSCWebConsoleMessageQueue |

**Серверная версия Агента администрирования**

Вместе с Сервером администрирования на устройство будет установлена серверная версия Агента администрирования. Она входит в состав Сервера администрирования, устанавливается и удаляется в его составе и может взаимодействовать только с локально установленным Сервером администрирования. Настраивать параметры подключения Агента к Серверу администрирования не требуется: настройка реализована программно с учетом того, что компоненты установлены на одном компьютере. Серверная версия Агента администрирования устанавливается с теми же атрибутами и выполняет те же функции управления программами, что и стандартный Агент администрирования. На эту версию будет действовать политика группы администрирования, в которую включено клиентское устройство Сервера администрирования. Для серверной версии Агента администрирования создаются все задачи, предусмотренные для Агента администрирования, за исключением задачи смены Сервера.

Отдельная установка Агента администрирования на устройство с Сервером администрирования невозможна.

Вы можете просматривать свойства служб Сервера и Агента администрирования, а также следить за их работой при помощи стандартных средств администрирования Microsoft Windows – Управление компьютером\Службы. Информация о работе службы Сервера администрирования сохраняется в системном журнале Microsoft Windows на устройстве, где установлен Сервер администрирования, в отдельной ветви журнала событий Kaspersky Event Log.

Не рекомендуется вручную запускать и отключать службы и менять учетные записи в настройках служб. При необходимости вы можете поменять учетную запись службы Сервера администрирования с помощью утилиты klsrvswch.

**Учетные записи и группы пользователей**

По умолчанию инсталлятор Сервера администрирования создает следующие учетные записи:

- - KL-AK-*: учетная запись службы Сервера администрирования;
- - KlScSvc: учетная запись для прочих служб из состава Сервера администрирования;
- - KlPxeUser: учетная запись для развертывания операционных систем.

Если на этапе работы инсталлятора вы выбирали другие учетные записи для службы Сервера администрирования и прочих служб, то будут использованы указанные вами учетные записи.

На устройстве, где установлен Сервер администрирования, также автоматически создаются локальные группы безопасности KLAdmins и KLOperators, с их соответствующими наборами прав (см. стр. 675).

Не рекомендуется устанавливать Сервер администрирования на контроллере домена. Тем не менее, если вы устанавливаете Сервер администрирования на контроллер домена, то вы должны запустить программу установки с правами администратора домена. В этом случае программа установки автоматически создаст доменные группы безопасности KLAdmins и KLOperators. Если вы устанавливаете Сервер администрирования на устройство, которое не является контроллером домена, то вы должны запустить программу установки с правами локального администратора. В этом случае программа установки автоматически создаст локальные группы безопасности KLAdmins и KLOperators.

При настройке уведомлений по электронной почте вам может потребоваться завести учетную запись на почтовом сервере для ESMTP-аутентификации.

См. также:

Учетные записи для работы с СУБД.....218

## Удаление программы

Вы можете удалить Kaspersky Security Center стандартными средствами установки и удаления программ Microsoft Windows. Для удаления программы запускается мастер, в результате работы которого с устройства будут удалены все компоненты программы (включая плагины). Мастер откроет веб-страницу в вашем браузере, используемом по умолчанию, с опросом, в котором вы можете сообщить нам, почему вы решили прекратить использование Kaspersky Security Center. Если во время работы мастера вы не задали удаление папки общего доступа (Share), то после завершения всех связанных с ней задач вы можете удалить ее вручную.

После удаления программы в системной временной папке могут оставаться файлы.

Мастер удаления программы предложит вам сохранить резервную копию Сервера администрирования.

При удалении программы с операционных систем Microsoft Windows 7 и Microsoft Windows 2008 возможно преждевременное завершение работы мастера создания задачи удаления программы. Чтобы избежать этого, отключите в операционной системе службу контроля учетных записей (UAC) и повторно запустите удаление программы.

# Об обновлении предыдущей версии Kaspersky Security Center

Этот раздел содержит информацию о том, как обновить Kaspersky Security Center с предыдущей версии. Вы можете обновить Kaspersky Security Center разными способами, в зависимости от того, был ли установлен

Kaspersky Security Center локально (см. стр. 281) или на узлах отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 282).

Во время обновления недопустимо совместное использование СУБД Сервером администрирования и какой-либо другой программой.

При обновлении предыдущей версии Kaspersky Security Center все установленные плагины поддерживаемых программ "Лаборатории Касперского" сохраняются. Плагин Сервера администрирования и плагин Агента администрирования обновляются автоматически (как для Консоли администрирования, так и для Kaspersky Security Center 14.2 Web Console).

## В этом разделе



# Сценарий: Обновление Kaspersky Security Center и управляемых программ безопасности

В этом разделе описан основной сценарий обновления программы Kaspersky Security Center и управляемых программ безопасности.

Обновление Kaspersky Security Center и управляемых программ безопасности состоит из следующих этапов:

a. **Проверка требований к оборудованию и программному обеспечению**

   Убедитесь, что ваше оборудование соответствует требованиям, и установите необходимые обновления (см. стр. 69).

b. **Планирование ресурсов**

   Оцените, сколько дискового пространства занимает ваша база данных. Убедитесь, что на жестком диске имеется достаточно свободного места для хранения резервной копии данных (см. стр. 689) Сервера администрирования.

c. **Получение файла установки Kaspersky Security Center**

   Получите исполняемый файл для текущей версии Kaspersky Security Center и сохраните его на устройство, выполняющее роль Сервера администрирования. Ознакомьтесь с информацией о выпуске для версии Kaspersky Security Center, которую вы используете.

d. **Создание резервной копии предыдущей версии**

   С помощью утилиты резервного копирования и восстановления данных (см. стр. 693) создайте резервную копию данных Сервера администрирования. Вы также можете создать задачу резервного копирования (см. стр. 693).

   Рекомендуется экспортировать список установленных плагинов.

e. **Запуск установщика**

Запустите исполняемый файл для последней версии (см. стр. 281) Kaspersky Security Center. После запуска файла укажите, что была создана резервная копия, а также путь к ней. Будет выполнено восстановление данных из резервной копии.

f. **Обновление управляемых программ**

Можно обновить программу, если доступна новая версия. Ознакомьтесь со списком поддерживаемых программ "Лаборатории Касперского" и убедитесь, что ваша версия Kaspersky Security Center совместима с этой программой. Затем обновите программу, как описано в информации о выпуске.

**Результаты**

После завершения сценария обновления убедитесь, что новая версия Сервера администрирования успешно установлена в Консоли управления (MMC). В меню выберите **Справка** → **О Kaspersky Security Center**. Отобразится номер версии программы.

Убедитесь, что вы используете последнюю версию Сервера администрирования в Kaspersky Security Center 14.2 Web Console, в верхней части экрана нажмите значок параметров (  ) рядом с именем Сервера администрирования. В открывшемся окне свойств Сервер администрирования на закладке **Общие** выберите раздел **Общие**. Отобразится номер версии программы.

Если вам нужно восстановить данные Сервера администрирования, выполните действия, описанные в следующем разделе: Резервное копирование и восстановление данных в интерактивном режиме (см. стр. 693).

Если вы обновили управляемую программу безопасности, убедитесь, что она установлена правильно на управляемых устройствах. Дополнительную информацию см. в документации к этой программе.

# Обновление предыдущей версии Kaspersky Security Center

В следующем разделе описаны рекомендуемые этапы подготовки к обновлению: Обновление Kaspersky Security Center и управляемых программ безопасности (см. стр. 280).

Вы можете установить Сервер администрирования версии 14.2 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 11 (11.0.0.1131b)). При обновлении до версии 14.2 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если при установке Сервера администрирования возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

Если в сети установлен хотя бы один Сервер администрирования новой версии, вы можете обновить другие Серверы администрирования в сети с помощью задачи удаленной установки, в которой используется инсталляционный пакет Сервера администрирования (см. стр. 1038).

Если вы развернули отказоустойчивый кластер "Лаборатории Касперского", вы также можете обновить Kaspersky Security Center (см. стр. 282) на его узлах.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 14.2:*

1. Запустите исполняемый файл ksc_14.2_<номер сборки>_full_<язык локализации>.exe для версии 14.2 (вы можете загрузить этот файл с сайта "Лаборатории Касперского").

2. В открывшемся окне по ссылке **Установить Kaspersky Security Center** запустите мастер установки Сервера администрирования. Следуйте далее указаниям мастера.
3. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:
   - **положения и условия настоящего Лицензионного соглашения;**
   - **Политику конфиденциальности, которая описывает обработку данных.**

   Установка программы будет продолжена после установки обоих флажков. Мастер установки предложит вам создать резервную копию данных Сервера администрирования для ранних версий.

   Kaspersky Security Center поддерживает восстановление данных из резервной копии, сформированной более ранней версией Сервера администрирования.
4. Если вы хотите создать резервную копию данных Сервера администрирования, укажите это в открывшемся окне **Создание резервной копии Сервера администрирования**.

   Резервная копия данных создается утилитой klbackup. Эта утилита входит в состав дистрибутива программы и располагается в корне папки установки Kaspersky Security Center (см. стр. 692).
5. Установите Сервер администрирования версии 14.2, следуя указаниям мастера установки.

   Если появляется сообщение о том, что служба Kaspersky Security Center 14.2 Web Console занята, в окне мастера нажмите на кнопку **Пропустить**.

   Не рекомендуется прерывать работу мастера установки. Прерывание процесса обновления на стадии установки Сервера администрирования может привести к неработоспособности новой версии Kaspersky Security Center.
6. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования (см. стр. 361).

   Рекомендуется обновить Агент администрирования для Linux до той же версии, что и Kaspersky Security Center.

   После выполнения задачи удаленной установки версия Агента администрирования обновлена.

### См. также



## Обновление Kaspersky Security Center на узлах отказоустойчивого кластера "Лаборатории Касперского"

Вы можете установить Сервер администрирования версии 14.2 на каждый узел отказоустойчивого кластера "Лаборатории Касперского", где установлен Сервер администрирования более ранней версии (начиная с версии 13.2). При обновлении до версии 14.2 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если вы ранее устанавливали Kaspersky Security Center на устройства локально, вы также можете обновить Kaspersky Security Center (см. стр. 281) на этих устройствах.

► *Чтобы обновить Kaspersky Security Center на узле отказоустойчивого кластера "Лаборатории Касперского":*

1. Выполните следующие действия на активном узле кластера:
   a. запустите исполняемый файл ksc_14.2.<номер сборки>_full_<язык>.exe.

      Откроется окно с выбором программ "Лаборатории Касперского" для обновления. Перейдите по ссылке **Установить Сервер администрирования Kaspersky Security Center**, чтобы запустить мастер установки Сервера администрирования. Следуйте инструкциям мастера.

   b. Ознакомьтесь с Лицензионным соглашением и Политикой конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я подтверждаю, что полностью прочитал, понимаю и принимаю** установите флажки:

      - **положения и условия настоящего Лицензионного соглашения;**
      - **Политику конфиденциальности, которая описывает обработку данных.**

      Установите оба флажка, чтобы продолжить установку.

      Если вы не принимаете Лицензионное соглашение или Политику конфиденциальности, нажмите на кнопку **Отменить** для отмены обновления.

   c. В окне **Тип установки на кластер** выберите узел, для которого требуется обновить Kaspersky Security Center.

      Далее инсталлятор настраивает и завершает обновление Сервера администрирования. Во время обновления параметры Сервера администрирования изменить нельзя.
2. Выполните на пассивном узле отказоустойчивого кластера "Лаборатории Касперского" те же действия, что и на активном узле. Если вы выбрали параметр **Отказоустойчивый кластер Microsoft (установить на все узлы кластера)** в окне **Тип установки на кластер**, пропустите этот шаг.
3. Запустить кластер (см. стр. 258).

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера "Лаборатории Касперского".

# Первоначальная настройка Kaspersky Security Center

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center для первоначальной настройки.

## В этом разделе



## Руководство по усилению защиты

Руководство по усилению защиты адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security Center, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security Center.

В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;
- настройка безопасного подключения к Серверу Администрирования;
- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования и клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы.

Перед началом работы с Сервером администрирования, Kaspersky Security Center предложит вам ознакомиться с краткой версией Руководства по усилению защиты.

Обратите внимание, что вы не можете использовать Сервер администрирования, пока не подтвердите, что ознакомились с Руководством по усилению защиты.

► *Чтобы прочитать Руководство по усилению защиты:*

1. Откройте Консоль администрирования или Kaspersky Security Center 14.2 Web Console и войдите в консоль. Консоль проверяет, подтвердили ли вы, что прочитали текущую версию Руководства по усилению защиты.

   Если вы еще не читали Руководство по усилению защиты, откроется окно с его краткой версией.

2. Выполните одно из следующих действий:

   - Если вы хотите просмотреть краткую версию Руководства по усилению защиты в виде текстового документа, перейдите по ссылке **Открыть в новом окне**.
   - Если вы хотите просмотреть полную версию Руководства по усилению защиты (см. стр. 147), перейдите по ссылке **Открыть руководство по усилению защиты** в онлайн-справке.

3. После прочтения Руководства по усилению защиты установите флажок **Я подтверждаю, что полностью прочитал(а) и понимаю Руководство по усилению защиты** и нажмите на кнопку **Принять**.

Теперь вы можете работать с Сервером администрирования.

При появлении новой версии Руководства по усилению защиты Kaspersky Security Center предложит вам ее прочитать.

## Мастер первоначальной настройки Сервера администрирования

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

kaspersky

## См. также:



## В этом разделе



# О мастере первоначальной настройки

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастер первоначальной настройки Сервера администрирования позволяет создать минимальный набор необходимых задач и политик, настроить минимум параметров, загрузить и установить плагины для управляемых программ "Лаборатории Касперского" и создать инсталляционные пакеты для управляемых программ "Лаборатории Касперского". В процессе работы мастера вы можете внести в программу следующие изменения:

- Загрузить и установить плагины для управляемых программ. После завершения работы мастера первоначальной настройки список установленных плагинов управления отображается в разделе **Дополнительно → Информация об установленных плагинах управления программами** в окне свойств Сервера администрирования.
- Создать инсталляционные пакеты для управляемых программ "Лаборатории Касперского". После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых программ "Лаборатории Касперского" отображаются в списке **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.
- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования. После завершения работы мастера первоначальной настройки информация о лицензионных ключах отображается в списке **Сервер администрирования**

→ **Лицензии "Лаборатории Касперского"** и в разделе **Лицензионные ключи** окна свойств Сервера администрирования.

- Настроить взаимодействие с Kaspersky Security Network (KSN).
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger). После завершения работы мастера первоначальной настройки параметры почтовых уведомлений отображаются в разделе **Уведомления** в окне свойств Сервера администрирования.
- Настроить параметры обновлений и закрытия уязвимостей программ, установленных на устройствах.
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств. После завершения работы мастера первоначальной настройки созданные задачи отображаются в списке **Сервер администрирования** → **Задачи**, а политики, соответствующие плагинам управляемых программ, отображаются в списке **Сервер администрирования** → **Политики**.

Мастер первоначальной настройки создает политики для управляемых программ, таких как Kaspersky Endpoint Security для Windows, если такие политики не были созданы ранее для группы **Управляемые устройства**. Мастер первоначальной настройки создает задачи, если задач с такими же именами нет в группе **Управляемые устройства**.

В Консоли администрирования Kaspersky Security Center автоматически предлагает запустить мастер первоначальной настройки после первого запуска программы. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

## Запуск мастера первоначальной настройки Сервера администрирования

Программа автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► *Чтобы запустить мастер первоначальной настройки вручную:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла выберите пункт **Все задачи** → **Мастер первоначальной настройки Сервера администрирования**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера.

При повторном запуске мастера первоначальной настройки задачи и политики, созданные при предыдущем запуске мастера, не создаются повторно.

## Шаг 1. Настройка параметров прокси-сервера

Укажите параметры доступа Сервера администрирования к интернету. Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых программ "Лаборатории Касперского".

Выберите параметр **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

  Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя**

  Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

- **Пароль**

  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Вы можете настроить доступ в интернет (см. стр. 301) позднее без запуска мастера первоначальной настройки.

## Шаг 2. Выбор способа активации программы

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите код активации

  *Код активации* – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Код активации отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

  Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

  Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- Укажите файл ключа

  *Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

  Файл ключа отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

  Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

  Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- Отложите активацию программы

  Программа будет работать в режиме Базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования.

Если вы выбрали отложенную активацию программы, вы можете добавить лицензионный ключ (см. стр. 393) позже в любое время.

См. также:

Основной сценарий установки.....92

## Шаг 3. Выбор областей защиты и операционных систем

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления программами и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети. Выберите следующие параметры:

- **Области**

  Вы можете выбрать одну из следующих областей защиты:

  - **Рабочие станции** Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.
  - **Файловые серверы и системы хранения данных**. Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.
  - **Виртуальные среды**. Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.
  - **Банкоматы и POS-системы**. Выберите этот параметр, если вы хотите защитить встроенные системы с операционной системой Windows, например банкоматы (ATM).
  - **Промышленные сети**. Выберите этот параметр, если вы хотите контролировать данные безопасности в промышленной сети и с конечных устройств сети,

защищенных программами "Лаборатории Касперского".

- **Промышленные конечные точки**. Выберите этот параметр, если вы хотите защитить отдельные узлы промышленной сети.

- **Операционные системы**

Можно выбрать инсталляционные пакеты программ "Лаборатории Касперского" из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов (см. стр. 381) по следующим критериям:

- область защиты;
- тип загружаемого программного обеспечения (дистрибутив, утилита, плагин или веб-плагин);
- версия программы "Лаборатории Касперского";
- язык локализации программы "Лаборатории Касперского".

## Шаг 4. Выбор плагинов для управляемых программ

Выберите плагины для управляемых программ для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге (см. стр. 289) мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, выберите язык в раскрывающемся списке **Отображать язык Консоли администрирования**. Список плагинов включает в себя следующие графы:

- **Название программы**

Выбраны подключаемые модули в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия программы**

В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Язык локализации**

По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования**.

После выбора плагинов, их установка начинается автоматически в отдельном окне. Для установки некоторых плагинов вы должны принять условия Лицензионного соглашения. Прочитайте Лицензионное соглашения, выберите параметр **Я принимаю условия Лицензионного соглашения** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

После завершения установки, закройте окно установки.

Вы также можете выбрать плагин управления (см. стр. 381) позднее без запуска мастера первоначальной настройки.

## Шаг 5. Загрузка дистрибутивов и создание инсталляционных пакетов

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

В окне **Тип шифрования** выберите один из следующих типов шифрования:

- Strong encryption (AES256). Для этого типа шифрования используется 256-разрядный ключ.
- Lite encryption (AES56). Для этого типа шифрования используется 56-разрядный ключ.

Окно **Тип шифрования** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**, а в качестве платформы – **Microsoft Windows** (см. стр. 289).

После того, как вы выбрали тип шифрования, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.

В раскрывающемся списке **Отображать язык Консоли администрирования** можно выбрать языки для дистрибутива.

Для дистрибутивов управляемых программ может потребоваться установка определенной минимальной версии Kaspersky Security Center.

В списке вы можете выбрать дистрибутив любого типа шифрования, отличного от того, который вы выбрали в окне **Тип шифрования**. После того, как вы выбрали дистрибутив Kaspersky Endpoint Security для Windows, начинается загрузка дистрибутивов, соответствующих компонентам и платформам (см. стр. 289). Вы можете контролировать ход загрузки в графе **Состояние загрузки**. После завершения работы мастера первоначальной настройки инсталляционные пакеты Агента администрирования для Windows и управляемых программ "Лаборатории Касперского" отображаются в списке **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

Чтобы завершить загрузку некоторых дистрибутивов вы должны принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вы должны принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Выберите параметры, связанные с Лицензионным соглашением и Политикой конфиденциальности "Лаборатории Касперского", и нажмите на кнопку **Принять все**. Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. После завершения загрузки отображается статус **Создан инсталляционный пакет**. В дальнейшем инсталляционные пакеты можно использовать для развертывания программ "Лаборатории Касперского" на клиентских устройствах.

Вы можете создать инсталляционные пакеты (см. стр. 372) позднее без запуска мастера первоначальной настройки. В дереве Консоли администрирования перейдите в раздел **Сервер администрирования → Дополнительно → Удаленная установка → Инсталляционные пакеты**.

## Шаг 6. Настройка использования Kaspersky Security Network

Можно подключать репутационные базы Kaspersky Security Network (см. стр. 829), чтобы обеспечить более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повысить эффективность работы некоторых компонентов защиты, а также снизить вероятность ложных срабатываний.

Прочтите Положение о Kaspersky Security Network (KSN), которое отображается в окне. Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые программы, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network (см. стр. 829). Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые программы не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

Если вы загрузили плагин Kaspersky Endpoint Security для Windows, отобразятся оба положения о KSN: Положение о KSN для Kaspersky Security Center и Положение о KSN для Kaspersky Endpoint Security для Windows. Положения о KSN для других управляемых программ "Лаборатории Касперского", для которых были загружены плагины, отображаются в отдельных окнах и каждое из них необходимо принять (или отклонить) отдельно.

Настроить доступ Сервера администрирования к Kaspersky Security Network (KSN) (см. стр. 830) можно также далее в окне свойств Сервера администрирования в Консоли администрирования.

## Шаг 7. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры отправки уведомлений о событиях, регистрируемых при работе программ "Лаборатории Касперского" на управляемых устройствах. Эти параметры будут использоваться в качестве значений по умолчанию для Сервера администрирования.

Для настройки рассылки оповещений о возникающих событиях программ "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **SMTP-серверы**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес
- Имя устройства в сети Windows (NetBIOS-имя)
- DNS-имя SMTP-сервера

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. Если вы используете несколько SMTP-серверов, соединение с ними устанавливается через указанный коммуникационный порт. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят.

- **Параметры**

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**.

Вы также можете настроить уведомления о событии (см. стр. 316) позднее без запуска мастера первоначальной настройки.

## Шаг 8. Настройка параметров управления обновлениями

Настройте параметры работы с обновлениями программ, установленных на клиентских устройствах.

Вы можете настроить эти параметры, только если вы предоставили лицензионный ключ, который предусматривает возможности Системного администрирования.

В блоке параметров **Режим поиска и установки обновлений** вы можете выбрать один из режимов поиска и установки обновлений Kaspersky Security Center:

- **Поиск требуемых обновлений**

  Создается задача *Поиск уязвимостей и требуемых обновлений*.

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

В блоке параметров **Служба Windows Server Update Services** вы можете выбрать один из способов синхронизации обновлений:

- **Использовать источники обновлений, заданные в политике домена**
- **Использовать Сервер администрирования в роли WSUS-сервера**

Обновления Центра обновления Windows загружаются на клиентские устройства с Сервера администрирования. Задача *Выполнение синхронизации с Центром обновления Windows* и политика Агента администрирования создаются автоматически, если они не были созданы ранее.

Вы можете создать (см. стр. 413) задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки.

Чтобы использовать Сервер администрирования в качестве WSUS-сервера (см. стр. 494), вы должны создать задачу *Синхронизация обновлений Windows Update* и включить параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования (см. стр. 750).

## Шаг 9. Создание первоначальной конфигурации защиты

В окне **Создание первоначальной конфигурации защиты** отображается список политик и задач, созданных автоматически. Создаются следующие политики и задачи:

- политика Агента администрирования Kaspersky Security Center;
- политики для управляемых программ "Лаборатории Касперского", чьи плагины управления были установлены ранее (см. стр. 290);
- задача обслуживания Сервера администрирования;
- задача резервное копирование данных Сервера администрирования;
- задача Загрузка обновлений в хранилище Сервера администрирования;
- задача Поиск уязвимостей и требуемых обновлений;
- задача Установка обновлений.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

Если вы загрузили и установили плагин для Kaspersky Endpoint Security для Windows версии 10 Service Pack 1 и выше, до версии 11.0.1, во время создания политик и задач откроется окно первоначальной настройки доверенной зоны Kaspersky Endpoint Security для Windows. Программа предложит внести в доверенную зону проверенных "Лабораторией Касперского" поставщиков, чтобы исключить их программы из проверки для предотвращения случайной блокировки. Вы можете создать рекомендованные исключения сейчас или создать список исключений позже, выбрав в дереве консоли **Политики** → меню свойств Kaspersky Endpoint Security → **Продвинутая защита** → **Доверенная зона** → **Настройка** → **Добавить**. Список исключений проверки доступен для редактирования в любой момент дальнейшей работы с программой.

Работа с доверенной зоной выполняется средствами программы Kaspersky Endpoint Security для Windows. Подробные инструкции по выполнению операций и описание особенностей шифрования приведены в онлайн-справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm.

Для завершения первоначальной настройки доверенной зоны и возвращения к мастеру нажмите **ОК**.

Нажмите **Далее**. Кнопка станет доступна, когда все необходимые политики и задачи будут созданы.

Также можно создать необходимые задачи (см. стр. 413) и политики (см. стр. 430) позднее без запуска мастера первоначальной настройки.

## Шаг 10. Подключение мобильных устройств

Если ранее в параметрах мастера вы включили область защиты **Мобильные устройства** (см. стр. 289), укажите параметры подключения корпоративных мобильных устройств управляемой организацией. Если вы не включили область защиты **Мобильные устройства**, этот шаг будет пропущен.

На этом шаге мастера выполните следующие действия:

- Настройте порты подключения мобильных устройств.
- Настройте параметры аутентификации Сервера администрирования.
- Создайте сертификаты или управлять ими.
- Настройте выпуск, автоматическое обновление и шифрование сертификатов общего типа.
- Создайте правила перемещения мобильных устройств.

► *Чтобы настроить порты подключения мобильных устройств:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить порты**.

   Откроется окно свойств Сервера администрирования на разделе **Дополнительные порты**.
3. В разделе **Дополнительные порты** вы можете настроить параметры подключения мобильных устройств:
   - **SSL-порт для прокси-сервера активации**

     Номер SSL-порта для подключения Kaspersky Endpoint Security для Windows к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17000.
   - **Открыть порт для мобильных устройств**

     Открывается порт, по которому мобильные устройства будут подключаться к Серверу лицензирования. Вы можете задать номер порта и другие настройки в полях ниже.

     По умолчанию параметр включен.
   - **Порт для синхронизации мобильных устройств**

     Номер порта, по которому мобильные устройства подключаются к Серверу администрирования и обмениваются с ним информацией. По умолчанию установлен порт 13292.

     Вы можете назначить другой порт, если порт 13292 используется в каких-то других целях.
   - **Порт для активации мобильных устройств**

     Порт подключения Kaspersky Endpoint Security для Android к серверам активации "Лаборатории Касперского".

     По умолчанию установлен порт 17100.
   - **Открыть порт для устройств с защитой на уровне UEFI**

     Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.
   - **Порт для устройств с защитой на уровне UEFI**

     Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию установлен порт 13294.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

Вам потребуется настроить аутентификацию Сервера администрирования мобильными устройствами и аутентификацию мобильных устройств Сервером администрирования. Вы можете настроить архитектуру программы позже, независимо от мастера первоначальной настройки.

► *Чтобы настроить параметры аутентификации Сервера администрирования мобильными устройствами:*

1. Нажмите на кнопку **Настроить** справа от поля **Подключение мобильных устройств**.
2. В раскрывающемся списке выберите **Настроить аутентификацию**.

   Откроется окно свойств Сервера администрирования на разделе **Сертификаты**.
3. Выберите вариант аутентификации для мобильных устройств в блоке параметров **Аутентификация Сервера мобильными устройствами** и для устройств со встроенной защитой на уровне UEFI в блоке параметров **Аутентификация Сервера устройствами с защитой на уровне UEFI**.

   Аутентификация Сервера администрирования при обмене информацией с клиентскими устройствами выполняется на основании сертификата.

   По умолчанию выбрано использование сертификата, созданного при установке Сервера администрирования. При необходимости можно добавить новый сертификат.

► *Чтобы добавить новый сертификат (не обязательно):*

1. Выберите **Другой сертификат**

   Появится кнопка **Обзор**.
2. Нажмите на кнопку **Обзор**.
3. В появившемся окне настройте параметры сертификата:
   - **Тип сертификата**
   - Срок активации:
     - **Немедленно**

       Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

       Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.
     - **Через указанный срок (сут)**

       Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**

       Рекомендуется запланировать перевыпуск сертификатов заранее. Резервный сертификат должен быть загружен на мобильные устройства до истечения указанного периода. После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства, не имеющие резервного сертификата, не смогут подключиться к Серверу администрирования.
4. Вы можете нажать на кнопку **Свойства**, чтобы просмотреть параметры выбранного сертификата Сервера администрирования.

► Чтобы перевыпустить сертификат, выпущенный средствами Сервера администрирования:

1. Выберите **Сертификат выпущен средствами Сервера администрирования**.
2. Нажмите на кнопку **Перевыпустить**.
3. В открывшемся окне настройте следующие параметры:
   - Адрес подключения:
     - **Оставить адрес подключения прежним**

       Адрес Сервера администрирования, к которому подключаются мобильные устройства, останется прежним.

       По умолчанию этот вариант выбран.
     - **Изменить адрес подключения на**

       Если необходимо, чтобы мобильные устройства подключались по другому адресу, укажите в поле требуемый адрес.

       При изменении адреса подключения мобильных устройств необходимо выпустить новый сертификат. Старый сертификат будет недействительным на подключенных мобильных устройствах. Ранее подключенные устройства не смогут подключиться к Серверу администрирования и перестанут быть управляемыми.
   - Срок активации:
     - **Немедленно**

       Текущий сертификат будет заменен новым сертификатом сразу после нажатия на кнопку **ОК**.

       Ранее подключенные мобильные устройства не смогут подключиться к Серверу администрирования.
     - **Через указанный срок (сут)**

       Если выбран этот вариант, то будет сгенерирован резервный сертификат. Текущий сертификат будет заменен новым сертификатом через указанное количество дней. Дата, с которой резервный сертификат вступит в силу, отображается в разделе **Сертификаты**

       Рекомендуется запланировать перевыпуск сертификатов заранее. Резервный сертификат должен быть загружен на мобильные устройства до истечения указанного периода. После того как текущий сертификат будет заменен новым сертификатом, ранее подключенные мобильные устройства, не имеющие резервного сертификата, не смогут подключиться к Серверу администрирования.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну **Сертификаты**.
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к мастеру первоначальной настройки.

► *Чтобы настроить выпуск, автоматическое обновление и шифрование сертификатов общего типа для идентификации мобильных устройств Сервером администрирования:*

1. Нажмите на кнопку **Настроить** справа от поля **Аутентификация мобильных устройств**.

   Откроется окно **Правила выпуска сертификатов** на разделе **Выпуск мобильных сертификатов**.

2. При необходимости настройте следующие параметры в блоке параметров **Параметры выпуска**:

   - **Срок действия сертификата, дней**

     Срок действия сертификата в днях. По умолчанию срок действия сертификата равен 365 дням. По истечении этого срока мобильное устройство не сможет подключаться к Серверу администрирования.

   - **Источник сертификата**

     Выбор источника сертификатов общего типа для мобильных устройств: сертификаты выпускает Сервер администрирования или сертификаты задаются вручную.

   Вы можете изменить шаблон сертификата, если в разделе **Интеграция с PKI** настроена интеграция с инфраструктурой открытых ключей. В этом случае будут доступны следующие поля выбора шаблона:

   - **Шаблон по умолчанию**

     Использование сертификата, выпущенного внешним источником сертификатов – центром сертификации – по шаблону, заданному по умолчанию.

     По умолчанию выбран этот вариант.

   - **Другой шаблон**

     Выбор шаблона, на основании которого будут выпускаться сертификаты. Шаблоны сертификатов можно задать в домене. По кнопке **Обновить список** можно обновить список шаблонов сертификатов.

3. При необходимости задайте следующие параметры автоматического выпуска сертификатов в блоке параметров **Параметры автоматического обновления**:

   - **Обновлять, когда до истечения срока действия осталось (сут)**

     Количество дней до истечения срока действия текущего сертификата, за которое Сервер администрирования должен выпустить новый сертификат. Например, если в поле указано значение 4, Сервер администрирования выпустит новый сертификат за четыре дня до окончания срока действия текущего сертификата. По умолчанию указано значение 7.

   - **Автоматически перевыпускать сертификат, если это возможно**

     Выберите этот параметр, чтобы автоматически перевыпускать сертификат за такое количество дней до его окончания срока действия, какое указано в поле **Обновлять, когда до истечения срока действия осталось (сут)**. Если сертификат был задан вручную, его нельзя обновить автоматически и включенный параметр не будет работать.

По умолчанию параметр выключен.

Сертификаты обновляются автоматически центром сертификации.

1. При необходимости настройте параметры расшифровки сертификатов при установке в блоке параметров **Защита паролем**.

   Выберите параметр **Запрашивать пароль при установке сертификата**, чтобы при установке сертификата на мобильное устройство у пользователя запрашивался пароль. Пароль используется только один раз, при установке сертификата на мобильное устройство.

   Пароль будет автоматически сгенерирован средствами Сервера администрирования и отправлен по указанному вами адресу электронной почты. Вы можете указать адрес электронной почты

пользователя либо свой собственный, если хотите затем передать пользователю пароль другим способом.

Вы можете указать количество символов пароля для расшифровки сертификата с помощью ползунка.

Функция запроса пароля необходима, например, для защиты общего сертификата в автономном пакете установки Kaspersky Endpoint Security для Android. Защита паролем не позволит злоумышленнику получить доступ к общему сертификату при краже автономного инсталляционного пакета с Веб-сервера Kaspersky Security Center.

Если параметр выключен, расшифровка сертификата при установке будет проводиться автоматически и у пользователя не будет запрашиваться пароль. По умолчанию параметр выключен.

2. Нажмите на кнопку **ОК**, чтобы сохранить изменения и вернуться к окну мастера первоначальной настройки.

   Нажмите на кнопку **Отмена**, чтобы вернуться к мастеру первоначальной настройки без сохранения внесенных изменений.

► *Чтобы включить функцию перемещения мобильных устройств в нужную вам группу администрирования,*

В поле **Автоматически перемещать мобильные устройства** включите параметр **Создать правило перемещения мобильных устройств**.

Если параметр **Создать правило перемещения мобильных устройств** включен, программа автоматически создает правило перемещения, которое перемещает устройства под управлением операционных систем Android и iOS в группу **Управляемые устройства**.

- с операционными системами Android, на которых установлен Kaspersky Endpoint Security для Android и мобильный сертификат;
- с операционными система iOS, на которых установлен iOS MDM-профиль с общим сертификатом.

Если такое правило уже существует, то программа не создает правило.

По умолчанию параметр выключен.

"Лаборатория Касперского" больше не поддерживает Kaspersky Safe Browser.

## Шаг 11. Загрузка обновлений

Обновления антивирусных баз для Kaspersky Security Center и управляемых программ "Лаборатории Касперского" загружаются автоматически. Обновления загружаются с серверов "Лаборатории Касперского".

Чтобы загружать обновления без запуска мастера первоначальной настройки, создайте и настройте (см. стр. 461) задачу *Загружать обновления в хранилище Сервера администрирования*.

## Шаг 12. Обнаружение устройств

В информационном окне **Опрос сети** отображается информация о статусе опроса сети Сервером администрирования.

Вы можете просмотреть обнаруженные в сети Сервером администрирования устройства и получить справку по работе с окном **Обнаружение устройств** по ссылкам в нижней части окна.

Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. Используйте Консоль администрирования для настройки опроса Windows-доменов (см. стр. 326), Active Directory (см. стр. 329), IP-диапазонов (см. стр. 331) и IPv6-сетей (см. стр. 333).

### См. также:


Сценарий: Обнаружение устройств в сети ..... 324

Основной сценарий установки ..... 92


### Шаг 13. Завершение работы мастера первоначальной настройки

В окне завершения работы мастера первоначальной настройки установите флажок **Запустить мастер удаленной установки**, если вы хотите запустить автоматическую установку антивирусных программ и/или Агента администрирования на устройства в вашей сети.

Для завершения работы мастера нажмите на кнопку **Готово**.

## Настройка подключения Консоли администрирования к Серверу администрирования

Консоль администрирования подключена к Серверу администрирования через SSL-порт TCP 13291. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

► *Чтобы разрешить подключение Консоли администрирования по порту 13000:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.
2. Перейдите в раздел:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Для ключа LP_ConsoleMustUsePort13291 (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 1.

4. Перезапустите службу Сервера администрирования.

В результате Консоль администрирования сможет подключаться к Серверу администрирования, используя порт 13000.

## Настройка параметров доступа Сервера администрирования к интернету

Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых программ "Лаборатории Касперского".

► *Чтобы указать параметры доступа Сервера администрирования к интернету:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Дополнительно** → **Параметры доступа к сети интернет**.
4. Выберите параметр **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

   - Номер порта

     Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

   - Не использовать прокси-сервер для локальных адресов

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - Аутентификация на прокси-сервере

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

     Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

   - Имя пользователя

     Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

   - Пароль

     Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки (см. стр. 287).

kaspersky

# Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

## В этом разделе



## Сценарий: Подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

### Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

### Этапы

Этот сценарий состоит из следующих этапов:

a. **Выбор клиентского устройства в демилитаризованной зоне**

   Это устройство будет использоваться в качестве шлюза соединения (см. стр. 90). Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

b. **Установка Агента администрирования в роли шлюза соединения**

   Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку (см. стр. 205).

   По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>

   При установке Агента администрирования в окне мастера установки **Шлюз соединений** выбрать вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

   Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения (см. стр. 663).

Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux (см. стр. 935).

**c. Разрешение соединения на сетевом экране шлюза соединения**

Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранах между Сервером администрирования и шлюзом соединения.

Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

**d. Создание группы администрирования для внешних устройств**

Создайте группу (см. стр. 709) внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

**e. Подключение шлюза соединения к Серверу администрирования**

Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

Добавьте шлюз соединения в качестве точки распространения (см. стр. 664).

Переместите шлюз соединения (см. стр. 724) из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

**f. Подключение внешних настольных компьютеров к Серверу администрирования**

Обычно внешние настольные компьютеры не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения (см. стр. 306) к Серверу администрирования через шлюз соединения при установке Агента администрирования.

**g. Настройка обновлений для внешних настольных компьютеров**

Если обновления программ безопасности настроены на загрузку с Сервера администрирования, внешние компьютеры загружают обновления через шлюз соединения, что имеет два недостатка. Это имеет два недостатка:

Это лишний трафик, занимающий пропускную способность интернет-канала компании.

Это не обязательно самый быстрый способ получать обновления. Возможно для внешних компьютеров будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

Выполните следующие действия:

Переместите все внешние компьютеры в отдельную группу администрирования, (см. стр. 724) которую вы создали ранее.

Исключить группу с внешними устройствами из задачи обновления (см. стр. 473).

Создайте отдельную задачу обновления для группы с внешними устройствами (см. стр. 473).

**h. Подключение ноутбуков к Серверу администрирования**

Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

Вам необходимо настроить правила для автономных пользователей (см. стр. 310): профили подключения (см. стр. 308) и описания сетевых расположений (см. стр. 311). Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

### См. также:

Доступ в интернет:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне .....166

## О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать программы безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).

  См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения (см. стр. 129)

- Сервер администрирования в демилитаризованной зоне (DMZ)

  См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете (см. стр. 132)

#### Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения в демилитаризованной зоне (см. стр. 90). Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети инициирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.

- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

**Сервер администрирования в демилитаризованной зоне (DMZ)**

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.
- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вы должны решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.
- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.
- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

См. также:



## Подключение внешних настольных компьютеров к Серверу администрирования

Настольные компьютеры, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

► *Чтобы подключить внешние настольные компьютеры к Серверу администрирования:*

1. Создание инсталляционного пакета Агента администрирования (см. стр. 372).
2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Дополнительно** и включите параметр **Подключаться к Серверу администрирования через шлюз соединений**.

   Параметр **Подключаться к Серверу администрирования через шлюз соединений** несовместим с параметром " **Использовать Агент администрирования в качестве шлюза соединений в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединений**.

   Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.

4. Создайте автономный инсталляционный пакет (см. стр. 374) на основе созданного инсталляционного пакета.
5. Доставьте автономный инсталляционный пакет на целевые компьютеры в электронном виде или на съемном диске.
6. Установите Агент администрирования из автономного инсталляционного пакета.

К Серверу администрирования подключены внешние настольные компьютеры.

## О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

**Использование различных адресов одного и того же Сервера администрирования**

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Подключения**, вложенный раздел **Профили соединений**). В окне создания профиля необходимо выключить параметр **Использовать только для получения обновлений** и включить параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне (см. стр. 166)), в профиле подключения следует указать адрес шлюза соединений в соответствующем поле.

**Переключение между Серверами администрирования в зависимости от текущей сети**

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и включите либо выключите параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

## См. также:

Доступ в интернет:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне .....166

Создание профиля соединения для автономных пользователей .....308

kaspersky

## Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► *Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:*

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать профиль подключения Агента администрирования к Серверу.
2. Выполните одно из следующих действий:
   - Если вы хотите создать профиль подключения для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
   - Если вы хотите создать профиль подключения для выбранного устройства в составе группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:
     a. Откройте окно свойств выбранного устройства.
     b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.
     c. Откройте окно свойств Агента администрирования.
3. В окне свойств в разделе **Подключения** выберите вложенный раздел **Профили соединений**.
4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

   По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

   В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах программы используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

   В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.
5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:
   - **Имя профиля**

     В поле ввода можно просмотреть или изменить имя профиля подключения.
   - **Адрес SMTP-сервера**

     Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.
   - **Номер порта**

     Номер порта, по которому будет выполняться подключение.
   - **Номер SSL-порта**

Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL**

  Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

  По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- По ссылке **Настроить подключение через прокси-сервер** настройте параметры профиля подключения через прокси-сервер: Выберите параметр **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

  - **Адрес**

    Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

    Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

  - **Имя пользователя** (поле доступно, если выбран параметр **Аутентификация на прокси-сервере**)

    Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  - **Пароль** (поле доступно, если включен параметр **Аутентификация на прокси-сервере**)

    Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

    Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

- **Адрес шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.

- **Включить автономный режим**

  Если параметр включен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. стр. 310). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

  Если параметр выключен, программы будут использовать активные политики.

По умолчанию параметр выключен.

- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений программами, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию параметр включен.

- Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле

  Если этот параметр включен, Агент администрирования подключается к Серверу администрирования, используя параметры, указанные в свойствах профиля.

  Если этот параметр выключен, Агент администрирования подключается к Серверу, используя исходные параметры, указанные при установке.

  Параметр доступен, если параметр **Использовать только для получения обновлений** выключен.

  По умолчанию параметр выключен.

6. Включите параметр **Включить автономный режим, когда Сервер администрирования недоступен**, чтобы при подключении программы, установленные на клиентском устройстве, использовали профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. стр. 310), если Сервер администрирования недоступен. В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль программы, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

### См. также:

О профилях соединения для автономных пользователей .....306

## О переключении Агента администрирования на другой Сервер администрирования

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. Для переключения Агента администрирования на другие Серверы администрирования можно использовать правила переключения (см. стр. 311). Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS (см. стр. 69).

Правила переключения могут срабатывать при изменении следующих параметров сети:

- Адрес шлюза соединений по умолчанию.
- IP-адрес DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
- DNS-суффикс подсети.
- IP-адрес DNS-сервера в сети.

- Доступность домена Windows. Этот параметр доступен только для устройств с операционными системами Windows.
- Адрес и маска подсети.
- IP-адрес WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- DNS-имя или NetBIOS-имя клиентского устройства.
- Доступность адреса SSL-соединения.

Если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение параметров сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах программы переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах программы возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** (см. стр. 308) включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

### См. также

Создание правила активации профиля политики.....441

## Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► *Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:*

1. В дереве консоли выберите группу администрирования, для устройств которой требуется создать правило переключения Агента администрирования по описанию сетевого местоположения.

2. Выполните одно из следующих действий:

   - Если вы хотите создать правило для всех устройств группы, в рабочей области группы на закладке **Политики** выберите политику Агента администрирования. Откройте окно свойств выбранной политики.
   - Если вы хотите создать правило для выбранного устройства группы, в рабочей области группы на закладке **Устройства** выберите устройство и выполните следующие действия:

     a. Откройте окно свойств выбранного устройства.

     b. В разделе **Программы** окна свойств устройства выберите Агент администрирования.

     c. Откройте окно свойств Агента администрирования.

3. В открывшемся окне свойств в разделе **Подключения** выберите вложенный раздел **Профили соединений**.
4. В блоке **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
5. В открывшемся окне **Новое описание** настройте параметры описания сетевого местоположения и правила переключения. Настройте следующие параметры описания сетевого местоположения:

   - **Имя описания сетевого местоположения**

     Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\/:|).

   - **Использовать профиль подключения**

     В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на политики для автономных пользователей. Профиль используется только для загрузки обновлений.

6. В блоке **Условия переключения** нажмите на кнопку **Добавить**, чтобы сформировать список условий описания сетевого местоположения.

   Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В раскрывающемся списке выберите значение, соответствующее изменению характеристики сети, к которой подключено клиентское устройство:

   - **Адрес основного шлюза** – изменение основного шлюза сети.
   - **Адрес DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
   - **Нахождение в DNS-домене** – изменение DNS-суффикса подсети.
   - **Адрес DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
   - **Доступность Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Используйте этот параметр только для устройств с операционными системами Windows.
   - **Нахождение в подсети** – изменение адреса и маски подсети.

- **Адрес WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Используйте этот параметр только для устройств с операционными системами Windows.
- **Разрешимость имен** – NetBIOS-имя клиентского устройства или DNS-имя было изменено.
- **Доступность адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

8. В открывшемся окне укажите значение условия переключения Агента администрирования на другой Сервер администрирования. Название окна зависит от выбора значения на предыдущем шаге. Настройте следующие параметры условия переключения:

   - **Значение**

     В поле можно добавить одно или несколько значений для создаваемого условия.

   - **Соответствует хотя бы одному значению списка**

     Если выбран этот вариант, условие будет выполняться при любом из значений, указанных в списке **Значение**.

     По умолчанию выбран этот вариант.

   - **Не соответствует ни одному из значений списка**

     Если выбран этот вариант, условие будет выполняться, если его значение отсутствует в списке **Значение**.

9. В окне **Новое описание** включите параметр **Описание активно**, чтобы включить использование нового описания сетевого местоположения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

Описания сетевого местоположения проверяются на соответствие характеристикам сети в том порядке, в котором они представлены в списке. Если характеристики сети соответствуют нескольким описаниям, будет использоваться первое из них. Вы можете изменить порядок следования правил в списке с помощью кнопок **Вверх** (  ) и **Вниз** (  ).

## Шифрование подключения SSL/TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием SSL/TLS. Вы можете включить SSL/TLS на Сервере администрирования и на Сервере iOS MDM. Kaspersky Security Center поддерживает SSL v3, также как и Transport Layer Security (TLS v1.0, 1.1, и 1.2). Вы можете выбрать протокол шифрования и наборы шифрования. Kaspersky Security Center использует самоподписанные сертификаты. Дополнительная настройка для iOS устройств не требуется. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные аккредитованным центром сертификации.

**Сервер администрирования**

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования:*

1. Используйте утилиту klscflag, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования. Введите следующую команду в командной строке Windows с правами администратора:

```
klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
```

Укажите параметр <value> команды:

- 0 – все разрешенные протоколы шифрования и наборы шифрования включены.
- 1 – SSL v2 выключен.

  Наборы шифрования:

  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - SEED-SHA
  - CAMELLIA128-SHA
  - IDEA-CBC-SHA
  - RC4-SHA
  - RC4-MD5
  - DES-CBC3-SHA
- 2 – SSL v2 и SSL v3 выключены (значение указано по умолчанию).

  Наборы шифрования:

  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - SEED-SHA
  - CAMELLIA128-SHA
  - IDEA-CBC-SHA
  - RC4-SHA
  - RC4-MD5

- DES-CBC3-SHA

- `3` – только TLS v1.2.

  Наборы шифрования:

  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - CAMELLIA128-SHA

2. Перезапустите следующие службы Kaspersky Security Center:
   - Сервер администрирования
   - Веб-сервер
   - службу активации прокси-сервера.

**Сервер iOS MDM**

Соединение между iOS устройствами и Сервером iOS MDM зашифровано.

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере iOS MDM:*

1. Откройте системный реестр клиентского устройства, на котором установлен Сервер iOS MDM, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset

   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
3. Создайте ключ с именем `StrictSslSettings`.
4. Укажите тип ключа `DWORD`.
5. Установите значение ключа:
   - `2` – без ограничений (разрешены TLS 1.0, TLS 1.1, TLS 1.2)
   - `3` – только TLS 1.2 (значение указано по умолчанию)
6. Перезапустите службу Сервера iOS MDM Kaspersky Security Center.

kaspersky

# Уведомления о событиях

В этом разделе описано, как выбрать способ уведомления администратора о событиях на клиентских устройствах, а также как настроить параметры уведомления о событиях.

Кроме того, описано, как проверить распространение уведомлений о событиях с помощью тестового "вируса" Eicar.

## В этом разделе



## Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений.

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. стр. 321).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно **Свойства: События**.
4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

   - **Электронная почта**

     На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес
- Имя устройства в сети Windows (NetBIOS-имя)
- DNS-имя SMTP-сервера

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

  Вы должны указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.
- Параметры TLS для SMTP-сервера:
  - **Не использовать TLS**

    Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.
  - **Использовать TLS, если поддерживается SMTP-сервером**

    Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.
  - **Всегда использовать TLS, проверить срок действия сертификата Сервера**

    Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для

аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого аккредитованного центра сертификации. Вы должны указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

  Вы должны указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

  Вы должны загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Программа отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны,

номера которых связаны с указанными адресами электронной почты.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес
- Имя устройства в сети Windows (NetBIOS-имя)
- DNS-имя SMTP-сервера

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

  Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера

  Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

- Выберите файл сертификата SMTP-сервера

  Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

Вы должны загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Программа отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

  По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

   Программа отправляет тестовое уведомление указанному получателю.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. стр. 748) или параметров программы (см. стр. 843).

## См. также:

Обработка и хранение событий на Сервере администрирования ..... 686

Сценарий: Мониторинг и отчеты ..... 576

## Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

► *Чтобы проверить распространение уведомлений о событиях:*

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Снова включите задачу постоянной защиты файловой системы.
2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с "вирусом" Eicar.

Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

В рабочей области узла **Сервер администрирования** на закладке **События** в выборке **Последние события** отобразится запись об обнаружении "вируса".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство программ безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR https://www.eicar.org.

## Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

*Таблица 54. Подстановочные параметры для описания события*

| Подстановочный параметр | Описание подстановочного параметра |
|---|---|
| %SEVERITY% | Уровень важности события |
| %COMPUTER% | Имя устройства, на котором произошло событие |
| %DOMAIN% | Доменная |
| %EVENT% | Событие |
| %DESCR% | Описание события |
| %RISE_TIME% | Время возникновения |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Имя задачи |
| %KL_PRODUCT% | Агент администрирования Kaspersky Security Center |
| %KL_VERSION% | Номер версии Агента администрирования |
| %HOST_IP% | IP-адрес; |
| %HOST_CONN_IP% | IP-адрес соединения |

**Пример:**

Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

## Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center:

- Отобразить и скрыть объекты в дереве консоли, рабочей области и окнах свойств объектов (папок, разделов) в зависимости от используемых функций.
- Отобразить и скрыть элементы главного окна (например, дерево консоли или стандартные меню, такие как **Действия** и **Вид**).

► *Чтобы настроить интерфейс Kaspersky Security Center в соответствии с используемым в настоящее время набором функций, выберите следующие действия:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В меню главного окна программы выберите пункт **Вид** → **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса**, настройте отображение элементов интерфейса, используя следующие флажки:
   - **Отображать Системное администрирование**

     Если этот параметр включен, в папке **Удаленная установка** отображается подпапка **Развертывание образов устройств**, а в папке **Хранилища** отображается подпапка **Оборудование**.

     Этот параметр по умолчанию выключен, если мастер первоначальной настройки не завершен. Этот параметр включен по умолчанию, если мастер первоначальной настройки завершен.
   - **Отображать шифрование и защиту данных**

     Если этот параметр включен, в дереве консоли отображается папка **Шифрование и защита данных**.

     По умолчанию параметр включен.
   - **Отображать параметры контроля рабочего места.**

     Если этот параметр включен, в разделе **Контроль безопасности** окна свойств Kaspersky Endpoint Security для Windows отображаются следующие подразделы:

     - **Контроль программ**
     - **Контроль устройств**
     - **Веб-Контроль.**
     - **Адаптивный контроль аномалий**

     Если этот параметр выключен, эти подразделы не отображаются в разделе **Контроль безопасности**.

     По умолчанию параметр включен.

- **Отображать Управление мобильными устройствами**

  Если этот параметр включен, возможности **Управления мобильными устройствами** доступны. После перезапуска программы в дереве консоли отображается папка **Мобильные устройства**.

  По умолчанию параметр включен.

- **Отображать подчиненные Серверы администрирования**

  Если флажок установлен, в дереве консоли отображаются узлы подчиненных и виртуальных Серверов администрирования в группах администрирования. При этом доступны функции, связанные с подчиненными и виртуальными Серверами администрирования, например, создание задач для удаленной установки программ на подчиненные Серверы администрирования.

  По умолчанию флажок снят.

- **Отображать разделы с параметрами безопасности**

  Если этот параметр включен, раздел **Безопасность** отображается в окне свойств Сервера администрирования, групп администрирования и других объектов. Этот параметр позволяет предоставить пользователям и группам пользователей настраиваемые права для работы с объектами.

  По умолчанию параметр выключен.

4. Нажмите на кнопку **ОК**.

Чтобы применить некоторые изменения, вы должны закрыть главное окно программы, а затем открыть его снова.

► *Чтобы настроить отображение элементов в главном окне программы:*

1. В меню главного окна программы выберите **Вид** → **Настроить**.
2. В открывшемся окне **Настройка вида** настройте отображение элементов главного окна с помощью флажков.
3. Нажмите на кнопку **ОК**.

# Обнаружение устройств в сети

В этом разделе описаны шаги, которые вы должны выполнить после установки Kaspersky Security Center.

## В этом разделе

kaspersky

# Сценарий: Обнаружение устройств в сети

Вы должны выполнить поиск устройств перед установкой программ безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

a. **Обнаружение устройств**

   Мастер первоначальной настройки выполняет начальное обнаружение устройств (см. стр. 299) и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную (см. стр. 325).

b. **Настройка расписания опросов**

   Определите, какой тип опроса (см. стр. 325) вы хотите регулярно использовать. Включите нужные типы опроса и настройте необходимое расписание опроса. Также см. рекомендации по частоте опроса сети.

c. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

   Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств (см. стр. 445), в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения (см. стр. 333).

   Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

**Результаты**

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

### См. также:



## Нераспределенные устройства

В этом разделе представлена информация о работе с устройствами сети организации, не входящими в группы администрирования.

### См. также:



### В этом разделе



### Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Включить опрос сети Windows**. Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удаться обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.

- **Опрос Active Directory**. Сервер администрирования получает информацию о структуре групп Active Directory, а также информацию о DNS-именах устройств, входящих в группы Active Directory. По умолчанию этот тип опроса включен. При использовании Active Directory рекомендуется использовать опрос Active Directory. В противном случае Сервер администрирования не сможет обнаружить устройства. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.
- **Опрос IP-диапазона**. Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и / или опрос Active Directory.
- **Опрос Zeroconf**. Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). По умолчанию этот тип опроса выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

Если вы настроили и включили правила перемещения устройств (см. стр. 445), новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес Active Directory или только определенный домен.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

## См. также:



## В этом разделе



# Опрос сети Windows

### Об опросе сети Windows

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- имя операционной системы;
- IP-адрес;
- DNS-имя;
- NetBIOS-имя.

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен.
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

**Просмотр и изменение параметров опроса сети Windows**

► *Чтобы изменить параметры опроса сети Windows:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

   В рабочей области подпапки **Домены** отображается список устройств.

2. Нажмите на кнопку **Опросить сейчас**.

   Откроется окно свойств домена. При необходимости настройте параметры опроса сети Windows:

   - **Включить опрос сети Windows**

     По умолчанию этот вариант выбран. Если не требуется выполнять опрос сети Windows (например, если достаточно опроса Active Directory), можно отменить выбор данного параметра.

   - **Настроить период быстрого опроса**

     По умолчанию интервал времени составляет 15 минут.

     При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети.

     Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждый N день**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию опрос запускается каждую пятницу в 18:00:00.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

- **Настроить период полного опроса**

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждый N день**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию опрос запускается каждую пятницу в 18:00:00.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Будут запущены оба типа опроса.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса сети Windows осуществляется в окне свойств точки распространения, в разделе **Обнаружение устройств**.

## См. также:

Работа с доменами Windows.Просмотр и изменение параметров домена .....333

Сценарий: Обнаружение устройств в сети.....324

## Опрос Active Directory

Используйте опрос Active Directory, если вы используете Active Directory; в противном случае рекомендуется использовать другие типы опросов. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

**Просмотр и изменение параметров опроса Active Directory**

► *Чтобы просмотреть и изменить параметры опроса групп Active Directory:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.

   Также вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. Нажмите на кнопку **Настроить параметры опроса**.

   В результате откроется окно свойств Active Directory. При необходимости настройте параметры опроса групп Active Directory:

- **Разрешить опрос Active Directory**

  По умолчанию этот вариант выбран. Однако если Active Directory не используется, в результаты опроса ничего найдено не будет. В этом случае можно отменить выбор данного параметра.

- **Настроить период опроса**

  По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

  Доступны следующие варианты расписания опроса сети:

  - **Каждый N день**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

  - **N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

  По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

  - **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию опрос запускается каждую пятницу в 18:00:00.

  - **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

  - **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

- **Дополнительно**

  Можно выбрать домены Active Directory для опроса:

  - Домен Active Directory, к которому относится Kaspersky Security Center.
  - Лес доменов, к которому относится Kaspersky Security Center.
  - Указанный список доменов Active Directory.

При выборе этого параметра можно добавлять домены в область опроса:

- Нажмите на кнопку **Добавить**.
- В соответствующих полях укажите адрес доменного контроллера, а также имя и пароль учетной записи для доступа к нему.
- Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Можно выбрать адрес доменного контроллера в списке и нажать на кнопку **Изменить** или **Удалить**, чтобы изменить или удалить его.

- Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса групп Active Directory осуществляются в окне свойств (см. стр.750) точки распространения, в разделе **Обнаружение устройств**.

## См. также:

Сценарий: Обнаружение устройств в сети.....324

## Опрос IP-диапазонов

Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и / или опрос Active Directory.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

### Просмотр и изменение параметров опроса IP-диапазонов

► *Чтобы просмотреть и изменить параметры опроса групп IP-диапазона:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

2. Если вы хотите, в подпапке **IP-диапазоны** нажмите на кнопку **Добавить подсеть**, чтобы добавить IP-диапазон (см. стр. 334) для опроса, а затем нажмите **ОК**.

3. Нажмите на кнопку **Настроить параметры опроса**.

   Откроется окно свойств IP-диапазонов. Если требуется, можно поменять параметры опроса IP-диапазонов:

   - **Разрешить опрос IP-диапазонов**

     По умолчанию этот вариант не выбран. Не рекомендуется использовать этот тип

опроса, если вы используете опрос сети Windows и/или опрос Active Directory.

- **Настроить период опроса**

  По умолчанию интервал времени составляет 420 минут. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

  Доступны следующие варианты расписания опроса сети:

  - **Каждый N день**

  Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

  По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

  - **N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

  По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

  - **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию опрос запускается каждую пятницу в 18:00:00.

  - **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

  - **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр включен.

Если требуется запустить опрос сети сразу, нажмите на кнопку **Опросить сейчас**. Эта кнопка доступна, только если выбран параметр **Разрешить опрос IP-диапазонов**.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса IP-диапазонов осуществляются в окне свойств (см. стр. 750) точки распространения, в разделе **Обнаружение устройств**. Клиентские устройства, найденные в результате опроса IP-диапазонов, отображаются в папке **Домены** виртуального Сервера.

### См. также:

Сценарий: Обнаружение устройств в сети.....324

### Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вы должны установить утилиту avahi-browse на точке распространения.

► *Чтобы включить опрос Zeroconf:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.
2. Нажмите на кнопку **Настроить параметры опроса**.
3. В открывшемся окне свойств IP-диапазонов выберите **Включить опрос с помощью технологии Zeroconf**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

## Работа с доменами Windows. Просмотр и изменение параметров домена

► *Чтобы изменить параметры домена:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.
2. Выберите домен и откройте окно его свойств одним из следующих способов:
   - В контекстном меню домена выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

   Откроется окно **Свойства: <Имя домена>** можно настроить параметры выбранного домена.

### См. также:

Сценарий: Обнаружение устройств в сети.....324

## Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Дополнительно** → **Обнаружение устройств** → **Домены**. Папка **Домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим

группам, которые были обнаружены во время опроса сети. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров опроса сети и работают, даже если опрос сети выключен.

► *Чтобы настроить правила хранения нераспределенных устройств:*

1. В дереве консоли в папке **Обнаружение устройств** выполните одно из следующих действий:
   - Чтобы настроить параметры родительской группы, в контекстном меню папки **Домены** выберите пункт **Свойства**.

     Откроется окно свойств родительской группы.
   - Чтобы настроить параметры дочерней группы, в контекстном меню дочерней группы выберите пункт **Свойства**.

     Откроется окно свойств дочерней группы.
2. В разделе **Устройства** укажите следующие параметры:
   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.
   - **Наследовать из родительской группы**

     Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

     Этот параметр доступен только для дочерних групп.

     По умолчанию параметр включен.
   - **Обеспечить принудительное наследование параметров для дочерних групп**

     Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

     По умолчанию параметр выключен.

Ваши изменения сохранены и применены.

### См. также:

Сценарий: Обнаружение устройств в сети.....324

## Работа с IP-диапазонами

Вы можете настраивать параметры существующих IP-диапазонов, а также создавать новые IP-диапазоны.

### См. также:

Сценарий: Обнаружение сетевых устройств ..... 324

### В этом разделе



## Создание IP-диапазона

► *Чтобы создать IP-диапазон:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. В контекстном меню папки выберите пункт **Новый** → **IP-диапазон**.
3. В открывшемся окне **Новый IP-диапазон** настройте параметры создаваемого IP-диапазона.

В результате созданный IP-диапазон появится в составе папки **IP-диапазоны**.

### См. также:

Сценарий: Обнаружение устройств в сети ..... 324

## Просмотр и изменение параметров IP-диапазона

► *Чтобы изменить параметры IP-диапазона:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **IP-диапазоны**.
2. Выберите IP-диапазон и откройте окно его свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

Откроется окно **Свойства: <Название IP-диапазона>** можно настроить параметры выбранного IP-диапазона.

### См. также:

Сценарий: Обнаружение устройств в сети ..... 324

## Работа с группами Active Directory. Просмотр и изменение параметров группы

► *Чтобы изменить параметры группы Active Directory:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Active Directory**.
2. Выберите группу Active Directory и откройте окно ее свойств одним из следующих способов:
   - В контекстном меню IP-диапазона выберите пункт **Свойства**.
   - По ссылке **Показать свойства группы**.

Откроется окно **Свойства: <Название группы Active Directory>** можно настроить параметры выбранной группы Active Directory.

См. также:

Сценарий: Обнаружение устройств в сети ..... 324

## Создание правил автоматического перемещения устройств в группы администрирования

Вы можете настроить автоматическое перемещение устройств, обнаруживаемых при опросе сети организации, в группы администрирования.

► *Чтобы настроить правила автоматического перемещения устройств в группы администрирования:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В рабочей области папки нажмите на кнопку **Настроить правила**.

Откроется окно **Свойства: Нераспределенные устройства**. Настройте правила автоматического перемещения устройств в группы администрирования в разделе **Перемещение устройств**.

На устройстве будет выполнено первое применимое правило в списке (сверху вниз в списке).

См. также:

Сценарий: Обнаружение устройств в сети ..... 324

## Использование динамического режима VDI на клиентских устройствах

В сети организации может быть развернута виртуальная инфраструктура с использованием временных виртуальных машин. Kaspersky Security Center обнаруживает временные виртуальные машины и добавляет данные о них в базу данных Сервера администрирования. После завершения работы пользователя с временной виртуальной машиной машина удаляется из виртуальной инфраструктуры. Однако запись об удаленной виртуальной машине может сохраниться в базе данных Сервера администрирования. Кроме того, несуществующие виртуальные машины могут отображаться в Консоли администрирования.

Чтобы избежать сохранения данных о несуществующих виртуальных машинах, в Kaspersky Security Center реализована поддержка динамического режима для Virtual Desktop Infrastructure (VDI). Администратор может включить поддержку динамического режима для VDI см. стр. 337) в свойствах инсталляционного пакета Агента администрирования (см. стр. 212), который будет установлен на временной виртуальной машине.

Во время выключения временной виртуальной машины Агент администрирования информирует Сервер администрирования о выключении. В случае успешного выключения виртуальной машины, она удаляется из списка устройств, подключенных к Серверу администрирования. Если выключение виртуальной машины выполнено некорректно и Агент администрирования не послал Серверу уведомление о выключении, используется дублирующий сценарий. Согласно этому сценарию виртуальная машина удаляется из списка устройств, подключенных к Серверу администрирования, после трех неудачных попыток синхронизации с Сервером.

kaspersky

## См. также:

Сценарий: Обнаружение сетевых устройств ..... 324

## В этом разделе



## Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

► *Чтобы включить динамический режим VDI:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства: Агент администрирования Kaspersky Security Center**.
3. В открывшемся окне **Свойства: Агент администрирования Kaspersky Security Center** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** включите параметр **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

## См. также:

Сценарий: Обнаружение устройств в сети ..... 324

## Поиск устройств, являющихся частью VDI

► *Чтобы найти устройства, являющиеся частью VDI:*

1. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
2. В окне **Поиск** на закладке **Виртуальные машины** в раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.
3. Нажмите на кнопку **Найти**.

Будет выполнен поиск устройств, являющихся частью Virtual Desktop Infrastructure.

## См. также:

Сценарий: Обнаружение устройств в сети ..... 324

### Перемещение в группу администрирования устройств, являющихся частью VDI

► *Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования:*

1. В рабочей области папки **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   В результате откроется окно свойств папки **Нераспределенные устройства**.

2. В окне свойств папки **Нераспределенные устройства** в разделе **Перемещение устройств** нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.

3. В окне **Новое правило** выберите раздел **Виртуальные машины**.

4. В раскрывающемся списке **Часть Virtual Desktop Infrastructure** выберите вариант **Да**.

Будет создано правило перемещения устройств в группу администрирования.

### См. также:

Сценарий: Обнаружение устройств в сети.....324

## Инвентаризация оборудования

В списке оборудования (**Хранилища** → **Оборудование**), который вы используете для инвентаризации оборудования, заполняется двумя способами: автоматически и вручную. После каждого опроса сети все обнаруженные компьютеры автоматически добавляются в список; однако вы также можете добавить компьютеры вручную, если не хотите опрашивать сеть. Вы можете добавить другие устройства в список вручную, например, маршрутизаторы, принтеры или компьютерное оборудование.

В свойствах устройства можно просматривать и редактировать подробную информацию об устройствах.

В списке оборудования могут присутствовать следующие типы устройств:

- компьютеры;
- мобильные устройства;
- сетевые устройства;
- виртуальные устройства;
- компьютерные комплектующие;
- компьютерная периферия;
- подключаемые устройства;
- VoIP-телефоны;
- сетевые хранилища.

Администратор может присваивать обнаруженным устройствам признак *Корпоративное оборудование*. Этот признак можно присвоить в свойствах устройства вручную или задать критерии для его автоматического присвоения. В этом случае признак *Корпоративное оборудование* присваивается по типу устройства.

Kaspersky Security Center позволяет выполнять списание оборудования. Для этого в свойствах устройства необходимо включить параметр **Устройство списано**. Такое устройство не отображается в списке оборудования.

Администратор может работать со списком программируемых логических контроллеров (ПЛК) в папке **Оборудование**. Подробная информация о работе со списками ПЛК приведена в *Руководстве пользователя Kaspersky Industrial CyberSecurity for Nodes*.

### См. также:



### В этом разделе



## Добавление информации о новых устройствах

► *Чтобы добавить информацию о новых устройствах в сети:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** по кнопке **Добавить устройство** откройте окно **Новое устройство**.

   Откроется окно **Новое устройство**.
3. В окне **Новое устройство** в раскрывающемся списке **Тип** выберите тип устройства, которое вы хотите добавить.
4. Нажмите на кнопку **ОК**.

   Откроется окно свойств устройства на разделе **Общие**.
5. В разделе **Общие** заполните поля ввода данными об устройстве. В разделе **Общие** доступны следующие параметры:
   - **Корпоративное устройство**. Установите флажок, если вы хотите присвоить устройству признак *Корпоративное*. По этому признаку можно выполнять поиск устройств в папке **Оборудование**.
   - **Устройство списано**. Установите флажок, если вы не хотите, чтобы устройство отображалось в списке устройств в папке **Оборудование**.
6. Нажмите на кнопку **Применить**.

Новое устройство отобразится в рабочей области папки **Оборудование**.

### См. также:



## Настройка критериев определения корпоративных устройств

► *Чтобы настроить критерии определения корпоративных устройств:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.

2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить критерии определения корпоративных устройств**.

   Откроется окно свойств оборудования.

3. В окне свойств оборудования в разделе **Корпоративные устройства** выберите способ присвоения устройству признака *Корпоративное*:

   - **Вручную устанавливать для устройства признак "Корпоративное"**. Признак *Корпоративное оборудование* назначается устройству вручную в окне свойств устройства в разделе **Общие**.
   - **Автоматически устанавливать для устройства признак "Корпоративное"**. В блоке параметров **По типу устройства** укажите типы устройств, которым программа будет автоматически присваивать признак *Корпоративное*.

     Этот параметр влияет только на те устройства, которые были добавлены с помощью опроса сети. Для устройств, добавленных вручную, установите параметр *Корпоративное* вручную.

4. Нажмите на кнопку **Применить**.

Критерии обнаружения корпоративных устройств настроены.

### См. также:

Сценарий: Обнаружение устройств в сети ..... 324

Инвентаризация оборудования ..... 338

## Настройка пользовательских полей

► *Чтобы настроить пользовательские поля устройств:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Оборудование**.
2. В рабочей области папки **Оборудование** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить пользовательские поля данных**.

   Откроется окно свойств оборудования.

3. В окне свойств оборудования в разделе **Пользовательские поля** нажмите на кнопку **Добавить**.

   Откроется окно **Добавить поле**.

4. В окне **Добавить поле** укажите название пользовательского поля, которое будет отображаться в свойствах оборудования.

   Вы можете создать несколько пользовательских полей с уникальными именами.

5. Нажмите на кнопку **Применить**.

В результате в свойствах оборудования в разделе **Пользовательские поля** будут отображаться добавленные пользовательские поля. Вы можете использовать пользовательские поля для указания специфической информации об устройствах. Например, номер внутренней заявки на приобретение оборудования.

### См. также:



# Лицензирование программы

В сертифицированном состоянии программы активация лицензии возможно только с использованием файла ключа.

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center.

### См. также:



### В этом разделе



## События превышения лицензионного ограничения

Kaspersky Security Center позволяет получать информацию о событиях превышения лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90%–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100%–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.

- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

### См. также:



## О лицензии

В этом разделе содержится информация о лицензировании программ "Лаборатории Касперского", управляемых с помощью Kaspersky Security Center.

### В этом разделе



### О лицензии

*Лицензия* – это ограниченное по времени право на использование программы, предоставляемое вам на основании Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование программы в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования программы зависят от типа лицензии, по которой была активирована программа.

Предусмотрены следующие типы лицензий:

- *Пробная.* Бесплатная лицензия, предназначенная для ознакомления с программой.

  Пробная лицензия имеет небольшой срок действия. По истечении срока действия пробной лицензии Kaspersky Security Center прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете активировать программу по пробной лицензии только один раз.

- *Коммерческая.* Платная лицензия, предоставляемая при приобретении программы.

  По истечении срока коммерческой лицензии ключевые функции программы отключатся. Чтобы продолжить использование Kaspersky Security Center, вам нужно продлить срок действия

коммерческой лицензии. Если вы не планируете продлевать лицензию, вам нужно удалить программу со своего компьютера.

Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить максимальную защиту от угроз компьютерной безопасности.

## О Лицензионном соглашении

*Лицензионное соглашение* – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Kaspersky Security Center и его компоненты, например Агент администрирования, имеют собственные Лицензионные соглашения.

Вы можете ознакомиться с условиями Лицензионного соглашения для Kaspersky Security Center следующими способами:

- Во время установки Kaspersky Security Center.
- Прочитав документ license.txt, включенный в комплект поставки Kaspersky Security Center.
- Прочитав документ license.txt в папке установки Kaspersky Security Center.
- Загрузив файл license.txt с сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.

Вы можете ознакомиться с условиями Лицензионного соглашения для Агента администрирования для Windows, Агента администрирования для Mac и Агента администрирования для Linux следующими способами:

- При загрузке дистрибутива Агента администрирования с веб-серверов "Лаборатории Касперского".
- При установке дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt, входящий в состав дистрибутива Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Прочитав документ license.txt в папке установки Агента администрирования для Windows, Агента администрирования для Mac или Агента администрирования для Linux.
- Загрузив файл license.txt с сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

## О лицензионном сертификате

*Лицензионный сертификат* – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

## О лицензионном ключе

*Лицензионный ключ* – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (резервным).

*Активный лицензионный ключ* – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

*Дополнительный (резервный) лицензионный ключ* – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

## О файле ключа

*Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- обратиться к продавцу лицензии;
- получить файл ключа на веб-сайте "Лаборатории Касперского" (https://keyfile.kaspersky.com/ru/) на основе имеющегося кода активации.

## О подписке

*Подписка на Kaspersky Security Center* – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании программы по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Если доступ к серверу через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871). Вы можете продлить подписку на веб-сайте поставщика услуг.

## О коде активации

*Код активации* – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить лицензионный ключ, активирующий Kaspersky Security Center. Вы получаете код активации по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871).

Если программа была активирована с помощью кода активации, в некоторых случаях после активации программа регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса лицензионного ключа. Для отправки запросов необходимо предоставить программе доступ в интернет.

Если вы потеряли код активации после установки программы, обратитесь к партнеру "Лаборатории Касперского", у которого вы приобрели лицензию.

Вы не можете использовать файлы ключей для активации управляемых программ; вы можете применить только коды активации.

### См. также:

Основной сценарий установки.....92

## Отзыв согласия с Лицензионным соглашением

Если вы решили прекратить защиту клиентских устройств, вы можете удалить управляемые программы "Лаборатории Касперского" и отозвать Лицензионное соглашение для этих программ.

► *Чтобы отозвать Лицензионное соглашение для управляемых программ "Лаборатории Касперского":*

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Принятые Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.
   - Ссылка на условия Лицензионного соглашения.
   - Список объектов, на которые распространяется Лицензионное соглашение: названия инсталляционных пакетов, имена обновлений, названия мобильных приложений.

3. Нажмите на кнопку **Отозвать Лицензионное соглашение**.

   В открывшемся окне отобразится информация о том, что необходимо удалить программу "Лаборатории Касперского", которой соответствует это Лицензионное соглашение.

4. Нажмите на кнопку, подтверждающую отзыв лицензии.

   Kaspersky Security Center проверяет, удалены ли инсталляционные пакеты, соответствующие управляемой программе "Лаборатории Касперского", Лицензионное соглашение которой вы отзываете.

   Можно отозвать только Лицензионное соглашение для управляемой программы "Лаборатории Касперского", для которой удален инсталляционный пакет.

Лицензионное соглашение отозвано. Оно больше не отображается в списке Лицензионных соглашений в разделе **Сервер администрирования → Дополнительно → Принятые Лицензионные соглашения**. Программу "Лаборатории Касперского", для которой было отозвано Лицензионное соглашение, больше нельзя использовать для защиты клиентских устройств.

### См. также

Сценарий: Настройка защиты сети ..... 400

## О предоставлении данных

**Данные, передаваемые третьим сторонам**

При использовании функциональности для управления мобильными устройствами Программным обеспечением с целью своевременной доставки команд на устройства под управлением операционной системы Android через механизм push-уведомлений используется Google Firebase Cloud Messaging. Если Пользователь настроил использование службы Google Firebase Cloud Messaging, Пользователь соглашается предоставить следующую информацию службе Google Firebase Cloud Messaging в автоматическом режиме: идентификаторы установки программ Kaspersky Endpoint Security для Android, на которые должны быть отправлены push-уведомления.

Чтобы блокировать обмен информацией со службой Google Firebase Cloud Messaging, Пользователь должен сбросить настройки использования службы Google Firebase Cloud Messaging.

При использовании функциональности для управления мобильными устройствами Программным обеспечением с целью своевременной доставки команд на устройства под управлением операционной системы iOS через механизм push-уведомлений, используется Apple Push Notification Service (APNs). Если Пользователь установил APNs-сертификат на сервер iOS MDM, сформировал iOS MDM-профиль с набором параметров подключения мобильных устройств iOS к Программному обеспечению и установил этот iOS MDM-профиль на мобильные устройства, Пользователь соглашается в автоматическом режиме предоставлять в APNs следующую информацию:

- Токен – push-токен устройства. Сервер использует этот токен при отправке push-уведомлений на устройство.
- PushMagic – строка, которая должна быть включена в push-уведомление. Значение строки генерируется устройством.

**Данные, обрабатываемые локально**

Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Kaspersky Security Center предоставляет администратору доступ к подробной информации об уровне безопасности сети организации и позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского". Kaspersky Security Center выполняет следующие основные функции:

- обнаружение устройств и их пользователей в сети организации;
- формирование иерархии групп администрирования для управления устройствами;
- установка программ "Лаборатории Касперского" на устройства;
- управление параметрами работы и задачами установленных программ;
- управление обновлениями программ "Лаборатории Касперского" и других производителей, поиск и закрытие уязвимостей;

- активация программ "Лаборатории Касперского" на устройствах;
- Управление учетными записями пользователей
- просмотр информации о работе программ "Лаборатории Касперского" на устройствах;
- просмотр отчетов.

Для выполнения своих основных функций программа Kaspersky Security Center может принимать, хранить и обрабатывать следующую информацию:

- Данные об устройствах в сети организации, полученные в результате обнаружения устройств в сети Active Directory, в сети Windows или сканирования IP-диапазонов. Сервер администрирования самостоятельно получает данные или передает Агенту администрирования.
- Данные Active Directory об организационных единицах, доменах, пользователях, группах, полученные в результате сканирования сети Active Directory. Сервер администрирования самостоятельно получает данные или передает Агенту администрирования.
- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейс Консоли администрирования или интерфейс Kaspersky Security Center 14.2 Web Console:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип Windows-домена, имя устройства в среде Windows, DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.
  - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств и для принятия решений о применимости тех или иных патчей и обновлений: состояние агента обновлений Windows (WUA), архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины; имя виртуального Сервера администрирования, который управляет устройствами; данные об облачном устройстве (облачный регион, VPC, облачная зона доступности, облачная подсеть, группа размещения облачного устройства).
  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.
  - Данные об учетных записях пользователей устройств и их сеансах работы.
- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.
- Параметры точки распространения, которые Пользователь вводит в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console.
- Данные, необходимые для подключения мобильных устройств к Серверу администрирования: сертификат, порт для подключения мобильных устройств, адрес подключения к Серверу администрирования. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center 14.2 Web Console.

- Данные о мобильных устройствах, передаваемые по протоколу Exchange ActiveSync. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:
  - Технические характеристики мобильного устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название операционной системы, номер IMEI и номер телефона.
  - Характеристики мобильного устройства и его компонентов: статус управления устройством, поддержка SMS, разрешение на отправку SMS-сообщений, поддержка FCM, поддержка пользовательских команд, папка хранения операционной системы и имя устройства.
  - Данные о действиях на мобильном устройствах: местоположение устройства (при использовании команды "Определить местоположение"), время последней синхронизации, время последнего подключения к Серверу администрирования и данные о поддержке синхронизации.
- Данные о мобильных устройствах, передаваемые по протоколу iOS MDM. Данные перечисленные ниже передаются от мобильного устройства Серверу администрирования:
  - Технические характеристики мобильного устройства и его компонентов, необходимые для идентификации устройства: имя устройства, модель, название и номер сборки операционной системы, номер модели устройства, номер IMEI, UDID, MEID, серийный номер, объем памяти, версия прошивки модема, MAC-адрес Bluetooth, MAC-адрес Wi-Fi и данные SIM-карты (код ICCID как часть идентификатора SIM-карты).
  - Данные о мобильной сети, используемой мобильным устройством: тип мобильной сети, название используемой мобильной сети, название домашней мобильной сети, версия параметров оператора мобильной сети, статус голосового роуминга и роуминга данных, код страны для домашней сети, код страны пребывания, код страны используемой сети и уровень шифрования.
  - Параметры безопасности мобильного устройства: использование пароля и его соответствие параметрам политики, список конфигурационных профилей и provisioning-профилей, используемых для установки сторонних приложений.
  - Дата последней синхронизации с Сервером администрирования и статус управления устройством.
- Данные о программах "Лаборатории Касперского", установленных на устройстве. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования:
  - Параметры программ "Лаборатории Касперского", установленных на управляемом устройстве: название и версия программы "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов программы, время последнего обновления и версия антивирусных баз, данные о параметрах и задачах программы "Лаборатории Касперского", информация об активных и резервных ключах, дата и идентификатор установки программы.
  - Статистика работы программы: события, связанные с изменениями статуса компонентов программы "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных программными компонентами.
  - Состояние устройства, определенное программой "Лаборатории Касперского".
  - Теги, передаваемые программой "Лаборатории Касперского".
  - Набор установленных и применимых обновлений к программе "Лаборатории Касперского".

- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.
- Данные, необходимые для интеграции Kaspersky Security Center с SIEM-системой для экспорта событий. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Настройки компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Настройки задач компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные:
  - Данные о программах и патчах, установленных на управляемых устройствах (Реестр программ).
  - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).
  - Данные об уязвимостях стороннего программного обеспечения, обнаруженных на управляемых устройствах.
  - Данные об обновлениях, доступных для сторонних программ, установленных на управляемых устройствах.
  - Данные об обновлениях Microsoft, найденные функцией WSUS.
  - Список обновлений Microsoft, найденных функцией WSUS, которые должны быть установлены на устройство.
- Данные, которые необходимы для загрузки обновлений на изолированный Сервер администрирования для закрытия уязвимостей в программах сторонних производителей на управляемых устройствах. Пользователь вводит и передает данные с помощью утилиты klscflag Сервера администрирования.
- Данные, необходимые для работы Kaspersky Security Center с облачным окружением (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Пользовательские категории программ. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль программ. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console. Полный список данных представлен в справке соответствующей программы.
- Данные о файлах, помещенных в резервное хранилище. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о файлах, находящихся на Карантине. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.

- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о состоянии и срабатывании правил Адаптивного контроля аномалий. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Информацию о шифровании устройств и статусах шифрования. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования.
- Данные об ошибках шифрования данных на устройствах, выполняемого функцией Шифрование данных программ "Лаборатории Касперского". Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Список управляемых программируемых логических контроллеров (ПЛК). Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные для создания цепочки развития угроз. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные, необходимые для интеграции Kaspersky Security Center со службой Kaspersky Managed Detection and Response (для Kaspersky Security Center 14.2 Web Console должен быть установлен специальный плагин): токен инициации интеграции, токен интеграции и токен сеанса пользователя. Пользователь с помощью токена инициации интеграции входит в интерфейс Kaspersky Security Center 14.2 Web Console. Служба Kaspersky MDR передает токен интеграции и токен сеанса пользователя через специальный плагин.
- Подробная информация о введенных кодах активации или указанных файлах ключей. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной номер телефона, пароль, секретный ключ, сгенерированный Сервером администрирования, и одноразовый пароль для двухэтапной проверки. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные, которые необходимы Identity and Access Manager для централизованной аутентификации и для обеспечения единого входа (SSO) между программами "Лаборатории Касперского", интегрированными с Kaspersky Security Center: параметры установки и конфигурации Identity и Access Manager, пользовательский сеанс Identity и Access Manager, токены Identity and Access Manager, статусы клиентских программ и статусы серверов ресурсов. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.

- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center 14.2 Web Console. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные, необходимые для работы плагинов управляемых программ в Kaspersky Security Center 14.2 Web Console и сохраняемые плагинами в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующей программы.
- Настройки пользователя Kaspersky Security Center 14.2 Web Console: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии нотификаций (прочитано / не прочитано), состояние столбцов в таблицах (скрыть / показать), прогресс прохождения режима обучения. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14.2 Web Console.
- Журнал событий Kaspersky Event Log для компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского". Журнал событий Kaspersky Event Log хранится на устройстве и никогда не передается на Сервер администрирования.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.
- Данные, необходимые для работы Kaspersky Security Center в облачных окружениях, таких как Amazon Web Services (AWS), Microsoft Azure, Google Cloud и Yandex.Cloud. Сервер администрирования получает данные от виртуальной машины, на которой он запущен.
- Информация о принятии Пользователем условий юридических соглашений с "Лабораторией Касперского".
- Данные Сервера администрирования, которые Пользователь вводит в следующих компонентах:
  - Консоль администрирования.
  - Kaspersky Security Center 14.2 Web Console.
  - Терминал командной строки при использовании утилиты klscflag.
  - Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Любые данные, которые Пользователь вводит в интерфейсе Консоли администрирования или Kaspersky Security Center 14.2 Web Console.

Перечисленные выше данные могут попасть в Kaspersky Security Center следующими способами:

- Пользователь вводит данные в интерфейс следующих компонентов:
  - Консоль администрирования.
  - Kaspersky Security Center 14.2 Web Console.
  - Терминал командной строки при использовании утилиты klscflag.
  - Компоненты, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut и OpenAPI Kaspersky Security Center.
- Агент администрирования самостоятельно собирает данные с устройства и передает на Сервер администрирования.

- Агент администрирования получает собранные управляемой программой "Лаборатории Касперского" данные и передает на Сервер администрирования. Перечни данных, обрабатываемых управляемыми программами "Лаборатории Касперского", приведены в справках соответствующих программ.
- Серверу администрирования и Агенту администрирования назначена точка распространения для получения информации о сетевых устройствах.
- Данные передаются с мобильного устройства на Сервер администрирования по протоколу Exchange ActiveSync или по протоколу iOS MDM.

Перечисленные данные хранятся в базе данных Сервера администрирования. Имена пользователей и пароли хранятся в зашифрованном виде.

Все перечисленные выше данные могут быть переданы "Лаборатории Касперского" только посредством файлов дампа, файлов трассировки или файлов журналов компонентов Kaspersky Security Center, включая файлы журналов, создаваемые инсталляторами и утилитами.

Файлы дампа, файлы трассировки и файлы журналов компонентов Kaspersky Security Center содержат случайные данные Сервера администрирования, Агента администрирования, Консоли администрирования, Сервера iOS MDM, Сервера мобильных устройств Exchange ActiveSync, Kaspersky Security Center 14.2 Web Console. Эти файлы могут содержать персональные и конфиденциальные данные. Файлы дампа, файлы трассировки и файлы журналов хранятся в открытой форме на устройстве. Файлы дампа, файлы трассировки и файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти данные в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

Переходя по ссылкам в Консоли администрирования или Kaspersky Security Center 14.2 Web Console, Пользователь соглашается на автоматическую передачу следующих данных:

- код Kaspersky Security Center;
- версия Kaspersky Security Center;
- локализация Kaspersky Security Center;
- идентификатор лицензии;
- тип лицензии;
- была ли приобретена лицензия через партнера.

Список данных, предоставляемых по каждой ссылке, зависит от цели и местоположения ссылки.

"Лаборатория Касперского" использует полученные данные в анонимной форме и только для целей общей статистики. Сводная статистика автоматически формируется из полученной исходной информации и не содержит каких-либо персональных или прочих конфиденциальных данных. При накоплении новых данных предыдущие данные уничтожаются (один раз в год). Сводная статистика хранится неограниченное время.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

## Варианты лицензирования Kaspersky Security Center

В Kaspersky Security Center лицензия может распространяться на разные группы функциональности.

При добавлении лицензионного ключа в окне свойств Сервера администрирования убедитесь, что вы добавили лицензионный ключ, который позволяет использовать Kaspersky Security Center. Вы можете найти

эту информацию на сайте "Лаборатории Касперского". На странице каждого решения есть список программ, включенных в это решение. Сервер администрирования может принимать неподдерживаемые лицензионные ключи, например лицензионный ключ для Kaspersky Endpoint Security Cloud, но функциональность Kaspersky Security Center в таких случаях не поддерживается.

**Базовая функциональность Консоли администрирования**

Доступны следующие функции:

- создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов;
- формирование иерархии групп администрирования для управления набором устройств как единым целым;
- контроль состояния антивирусной безопасности организации;
- удаленная установка программ;
- просмотр списка образов операционных систем, доступных для удаленной установки;
- централизованная настройка параметров программ, установленных на клиентских устройствах;
- просмотр и изменение существующих групп лицензионных программ;
- получение статистики и отчетов о работе программ, а также уведомлений о критических событиях;
- управление процессом шифрования и защиты данных;
- просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети;
- централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена;
- управление ролями пользователей.

Программа Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе программ "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования (см. стр. 356).

**Системное администрирование**

Доступны следующие функции:

- удаленная установка операционных систем;
- удаленная установка обновлений программного обеспечения, поиск и закрытие уязвимостей;
- инвентаризация оборудования;
- управление группами лицензионных программ;
- удаленное разрешение подключения к клиентским устройствам с помощью компонента Microsoft® Windows® "Подключение к удаленному рабочему столу";
- удаленное подключение к клиентским устройствам с помощью совместного доступа к рабочему столу Windows.

Единицей управления для Системного администрирования является клиентское устройство в группе "Управляемые устройства".

С использованием возможности Системного администрирования при инвентаризации доступны подробные сведения об оборудовании устройств. Для правильной работы Системного администрирования объем свободного места на жестком диске должен составлять не менее 100 ГБ.

**Управление мобильными устройствами**

Возможность Управления мобильными устройствами предназначена для управления мобильными устройствами Exchange ActiveSync и iOS MDM.

Для мобильных устройств Exchange ActiveSync доступны следующие функции:

- создание и редактирование профилей управления мобильными устройствами, назначение профилей почтовым ящикам пользователей;
- настройка параметров работы мобильного устройства (синхронизация почты, использование приложений, пароль пользователя, шифрование данных, подключение съемных дисков);
- установка сертификатов на мобильные устройства.

Для iOS MDM-устройств доступны следующие функции:

- создание и редактирование конфигурационных профилей, установка конфигурационных профилей на мобильные устройства;
- установка приложений на мобильное устройство через App Store® или с помощью манифест-файлов (.plist);
- возможность блокировать мобильное устройство, сбрасывать пароль мобильного устройства и удалять все данные с мобильного устройства.

С использованием возможности Управление мобильными устройствами доступно выполнение команд, предусмотренных соответствующими протоколами.

Единицей управления для Управления мобильными устройствами является мобильное устройство. Мобильное устройство считается управляемым, как только оно подключается к Серверу мобильных устройств.

**Управление доступом на основе ролей**

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых программ "Лаборатории Касперского".

Вы можете настроить права доступа к функциям программы для пользователей Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

**Установка операционных систем и программ**

Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ "Лаборатории Касперского" или других производителей программного обеспечения. Вы можете выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета. Вы можете использовать полученные образы для развертывания на новых

устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE).

**Интеграция с облачными окружениями**

Kaspersky Security Center не только работает с физическими устройствами, но также предоставляет возможность для работы в облачном окружении, например, с помощью настройки облачного окружения. Kaspersky Security Center работает со следующими виртуальными машинами:

- инстансы Amazon EC2;
- виртуальные машины Microsoft Azure;
- инстансы виртуальных машин Google Cloud.

**Экспорт событий в SIEM-системы: QRadar от IBM и Micro Focus от Micro Focus**

Экспорт событий можно использовать в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

По специальной лицензии протоколы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий, а также событий, переданных программами "Лаборатории Касперского" Серверу администрирования.

LEEF – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center.

CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа. SIEM-системы ArcSight и Splunk используют этот протокол.

### См. также:

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Лицензии и возможности Kaspersky Security Center .....69

## Об ограничениях базовой функциональности

До активации программы или по истечении срока действия коммерческой лицензии Kaspersky Security Center работает в режиме базовой функциональности Консоли администрирования. Далее приведено описание ограничений, которые накладываются на работу программы в этом режиме.

**Управление мобильными устройствами**

Невозможно создать новый профиль и назначить его мобильному устройству (iOS MDM) или почтовому ящику (Exchange ActiveSync). Изменение существующих профилей и их назначение почтовым ящикам доступно всегда.

**Управление программами**

Невозможно запустить задачи установки и удаления обновлений. Все задачи, запущенные до истечения срока действия лицензии, выполняются до конца, но последние обновления не устанавливаются. Например, если до истечения срока действия лицензии была запущена задача установки критических обновлений, то будут установлены только критические обновления, найденные до истечения срока действия лицензии.

Запуск и редактирование задач синхронизации, поиска уязвимостей и обновления базы уязвимостей доступны всегда. Ограничения также не накладываются на просмотр, поиск и сортировку записей в списке уязвимостей и обновлений.

**Дистанционная установка операционных систем и программ**

Невозможно запустить задачи снятия и установки образа операционной системы. Задачи, запущенные до истечения срока действия лицензии, выполняются до конца.

**Инвентаризация оборудования**

Недоступно получение информации о новых устройствах с помощью Сервера мобильных устройств. При этом информация о компьютерах и подключаемых устройствах обновляется.

Не работают оповещения об изменении конфигурации устройств.

Список оборудования доступен для просмотра и редактирования вручную.

**Управление группами лицензионных программ**

Невозможно добавить новый лицензионный ключ.

Не рассылаются оповещения о том, что превышены ограничения на использование лицензионных ключей.

**Удаленное подключение к клиентским устройствам**

Удаленное подключение к клиентским устройствам недоступно.

**Антивирусная безопасность**

Антивирус использует базы, установленные до истечения срока действия лицензии.

**Интеграция с облачными окружениями**

При работе в облачном окружении вы не можете использовать инструменты AWS, Azure или Google API для опроса облачных сегментов и установки программ на устройства. Недоступны также элементы интерфейса, отображающие функции, специфические для работы в облачном окружении.

## См. также:

Основной сценарий установки.....92

Лицензии и возможности Kaspersky Security Center.....69

# Особенности лицензирования Kaspersky Security Center и управляемых программ

Лицензирование Сервера администрирования и управляемых программ имеет следующие особенности:

- На Сервер администрирования можно добавить лицензионный ключ или действительный код активации (см. стр. 389) для активации возможностей Системного администрирования, Управления мобильными устройствами или интеграции с SIEM-системами. Некоторые функции Kaspersky Security

Center доступны только при наличии активных ключей или действительных кодов активации, добавленных на Сервер администрирования.

- В хранилище Сервера администрирования вы можете добавить несколько кодов активации и файлов ключей для управляемых программ (см. стр. 393).

**Особенности лицензирования Kaspersky Security Center**

Например, если вы активировали с помощью файла ключа одну из возможностей (например, Управления мобильными устройствами), но вам дополнительно потребовались другие возможности (например, Системного администрирования), в этом случае необходимо приобрести ключ, который активирует обе функциональности, и активировать этим ключом Сервер администрирования.

**Особенности лицензирования управляемых программ**

Для лицензирования управляемых программ вы можете распространить код активации или ключ автоматически или другим удобным для вас способом. Существуют следующие способы распространения кода активации или файла ключа:

- Автоматическое распространение

  Если вы используете разные управляемые программы и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

  Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Программа определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае нельзя предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

  При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, таким устройствам будет присвоен статус *Критический*.

- Добавление файла ключа или кода активации в инсталляционный пакет управляемой программы.

  В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этой программы. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

- Распространение с помощью задачи добавления лицензионного ключа управляемой программы

  В случае использования задачи добавления лицензионного ключа управляемой программы вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

- Добавление кода активации или файла ключа вручную на устройства.

См. также:



# Программы "Лаборатории Касперского". Централизованное развертывание

В этом разделе описаны способы удаленной установки программ "Лаборатории Касперского" и их удаления с устройств сети.

Перед началом установки программ на клиентские устройства требуется убедиться в том, что аппаратное и программное обеспечение устройств соответствует требованиям.

Связь Сервера администрирования с клиентскими устройствами обеспечивает Агент администрирования. Поэтому его необходимо установить на каждое клиентское устройство, которое будет подключено к системе удаленного централизованного управления. На устройстве, где установлен Сервер администрирования, может использоваться только серверная версия Агента администрирования. Она входит в состав Сервера администрирования и устанавливается и удаляется вместе с ним. Устанавливать Агент администрирования на это устройство не требуется.

Установка Агента администрирования осуществляется точно так же, как и установка программ, и может быть проведена как удаленно, так и локально. При централизованной установке программ безопасности через Консоль администрирования вы можете установить Агент администрирования совместно с программами безопасности.

Агенты администрирования могут отличаться в зависимости от программ "Лаборатории Касперского", с которыми они работают. В некоторых случаях возможна только локальная установка Агента администрирования (подробнее см. в Руководствах к соответствующим программам). Вам нужно установить Агент администрирования на клиентское устройство только один раз.

Управление программами "Лаборатории Касперского" (см. стр. 69) через Консоль администрирования выполняется при помощи плагинов управления. Поэтому для получения доступа к управлению программой через Kaspersky Security Center плагин управления этой программой должен быть установлен на рабочее место администратора.

Вы можете выполнить удаленную установку программ с рабочего места администратора в главном окне программы Kaspersky Security Center.

Для удаленной установки программного обеспечения следует создать задачу удаленной установки.

Сформированная задача удаленной установки будет запускаться на выполнение в соответствии со своим расписанием. Вы можете прервать процедуру установки, остановив выполнение задачи вручную.

Если удаленная установка программы завершается с ошибкой, вы можете проверить, чем вызвана эта проблема, и устранить ее с помощью утилиты подготовки устройства к удаленной установке (см. стр. 383).

Вы можете отслеживать процесс установки программ безопасности "Лаборатории Касперского" в сети с помощью отчета о развертывании.

Подробную информацию об управлении перечисленными программами через Kaspersky Security Center см. в Руководствах к соответствующим программам.

### В этом разделе



### См. также:



## Замещение программ безопасности сторонних производителей

Для установки программ безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Kaspersky Security Center предоставляет несколько способов удаления программ сторонних производителей.

**Удаление несовместимых программ с помощью программы установки**

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых программ поддерживается различными типами установки. Перед установкой программы безопасности несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета программы безопасности (раздел **Несовместимые программы**) включен параметр **Удалять несовместимые программы автоматически**.

**Удаление несовместимых программ при настройке удаленной установки программы**

Вы можете включить параметр **Удалять несовместимые программы автоматически** во время настройки удаленной установки программы безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В программе Kaspersky Security Center 14.2 Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые программы перед установкой программы безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Установка программ с помощью мастера удаленной установки (см. стр. 365).
- Kaspersky Security Center 14.2 Web Console: Удаление несовместимых программ перед установкой (см. стр. 1032).

**Удаление несовместимых программ с помощью отдельной задачи**

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы безопасности не может успешно удалить какую-либо из несовместимых программ.

Инструкции для Консоли администрирования: Создание задачи (см. стр. 413).

# Установка программ с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. стр. 383).

## В этом разделе



## Установка программы на выбранные устройства

► *Чтобы установить программу на выбранные устройства:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка программы**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.
3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные устройства.

## Установка программы на клиентские устройства группы администрирования

► *Чтобы установить программу на клиентские устройства группы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** выберите тип задачи **Удаленная установка программы**.

В результате работы мастера создания задачи будет создана групповая задача удаленной установки выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.

5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на клиентские устройства группы администрирования.

## Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory.

Установка программ с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory:*

1. Начните настройку установки программы с помощью мастера удаленной установки (см. стр. 365).
2. В окне мастера удаленной установки **Определение параметров задачи удаленной установки** выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. В окне мастера удаленной установки **Выбор учетных записей для доступа к устройствам** выберите параметр **Учетная запись требуется (установка без Агента администрирования)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.
5. Предоставьте разрешения выбранной учетной записи:
   a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.
   b. Нажмите на узел с нужным доменом.
   c. Нажмите на раздел **Делегирование**.
   d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.
   e. Нажмите на кнопку **Добавить**.
   f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.
   g. Нажмите на кнопку **ОК** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.
   h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.
   i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.
   j. Предоставьте следующие разрешения:

- **создание объектов группы;**
- **удаление объектов группы;**
- **создание объектов контейнера групповой политики;**
- **удаление объектов контейнера групповой политики.**

k. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

6. Задайте другие параметры, следуя инструкциям мастера.
7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
   - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
   - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).
2. Kaspersky Security Center устанавливает выбранные программы "Лаборатории Касперского" на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемой программы.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужной программы.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

### Установка программ на подчиненные Серверы администрирования

► *Чтобы установить программу на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если инсталляционного пакета нет на каком-либо из подчиненных Серверов, распространите его с помощью задачи распространения инсталляционного пакета (см. стр. 378).
3. Запустите создание задачи установки программы на подчиненные Серверы администрирования одним из следующих способов:
   - Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи удаленной установки для этой группы (см. стр. 362).
   - Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи удаленной установки для набора устройств (см. стр. 362).

   В результате запустится мастер создания задачи удаленной установки. Следуйте далее указаниям мастера.

   В окне **Выбор типа задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная установка программы на подчиненные Серверы администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет установлена на выбранные подчиненные Серверы администрирования.

## Установка программ с помощью мастера удаленной установки

Для установки программ "Лаборатории Касперского" вы можете воспользоваться мастером удаленной установки. Мастер удаленной установки позволяет проводить удаленную установку программ как с использованием сформированных инсталляционных пакетов, так и с дистрибутивов.

Для правильной работы задачи удаленной установки на клиентском устройстве, на котором не установлен Агент администрирования, необходимо открыть следующие порты: TCP 139 и 445; UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. стр. 383).

► *Чтобы установить программу на выбранные устройства с помощью мастера удаленной установки:*

1. В дереве консоли перейдите к папке **Удаленная установка** и выберите вложенную папку **Инсталляционные пакеты**.

2. В рабочей области папки выберите инсталляционный пакет программы, которую нужно установить.
3. В контекстном меню инсталляционного пакета выберите пункт **Установить программу**.

   Запустится мастер удаленной установки.
4. В окне **Выбор устройств для установки** можно сформировать список устройств, на которые будет установлена программа:

   - **Установить на группу управляемых устройств**

     Если выбран этот вариант, задача удаленной установки программы будет создана для группы устройств.

   - **Выбрать устройства для установки**

     Если выбран этот вариант, задача удаленной установки программы будет создана для набора устройств. В состав набора могут входить как устройства в составе групп, так и нераспределенные устройства.
5. В окне **Определение параметров задачи удаленной установки** настройте параметры удаленной установки программы.

   В блоке параметров **Принудительная загрузка инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки программы:

   - **С помощью Агента администрирования**

     Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

     Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

     Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

     По умолчанию параметр включен.

   - **Средствами Microsoft Windows с помощью Сервера администрирования**

     Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

     По умолчанию параметр включен.

   - **Средствами операционной системы с помощью точек распространения**

     Если этот параметр включен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

     Если включен параметр **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

     По умолчанию параметр включен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

   - **Количество попыток установки**

Если при запуске задачи удаленной установки Kaspersky Security Center не удается установить программу на управляемое устройство за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку установочного пакета на это управляемое устройство и больше не запускает установку на устройстве.

Параметр `Количество попыток установки` позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует установке. Администратор должен решить проблему в течение указанного количества попыток установки (например, выделив достаточно места на диске, удалив несовместимые программы или изменив параметры других программ, препятствующих установке), и перезапустить задачу (вручную или по расписанию).

Если установка не выполнена, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

Если количество попыток установки, указанное в параметрах задачи, было превышено и устройство готово к установке программы, вы можете увеличить значение параметра `Количество попыток установки` и запустить задачу по установке программы. Также вы можете создать другую задачу удаленной установки.

Определите, какое действие выполнять с клиентскими устройствами, управляемыми другим Сервером администрирования:

- **Устанавливать всегда**

  Программа устанавливается даже на устройства, управляемые другими Серверами администрирования.

  По умолчанию этот вариант выбран. Не нужно изменять этот параметр, если в вашей сети есть только один Сервер администрирования.

- **Устанавливать на устройства, управляемые только этим Сервером**

  Программа устанавливается только на устройства, которые управляются данным Сервером администрирования. Выберите этот параметр, если в вашей сети установлено больше одного Сервера администрирования и вы хотите избежать конфликтов (см. стр. 699) между ними.

Настройте дополнительные параметры:

- **Не устанавливать программу, если она уже установлена**

  Если этот параметр включен, выбранная программа не устанавливается заново, если она уже установлена на клиентском устройстве.

  Если этот параметр выключен, программа будет установлена в любом случае.

  По умолчанию параметр включен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

1. В окне **Выбор лицензионного ключа** выберите лицензионный ключ и способ его распространения:

- **Не помещать ключ в инсталляционный пакет (рекомендуется)**

  Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

  - если в свойствах ключа настроено автоматическое распространение (см. стр. 395);
  - если создана задача **Добавление ключа**.

- **Поместить ключ в инсталляционный пакет**

  Ключ распространяется на устройства вместе с инсталляционным пакетом.

Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

Окно **Выбор лицензионного ключа** отображается, если в состав инсталляционного пакета не входит лицензионный ключ.

Если в состав инсталляционного пакета входит лицензионный ключ, отображается окно **Свойства лицензионного ключа** с информацией о лицензионном ключе.

1. В окне **Выбор параметра перезагрузки операционной системы** определите, перезагружать ли устройства, если в ходе установки программ на них потребуется перезагрузка операционной системы:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки программы безопасности.

   - **Перезагрузить устройство**

     Если выбран этот вариант, устройство будет перезагружено после установки программы безопасности.

   - **Запрашивать у пользователя**

     Если выбран этот вариант, после установки программы безопасности пользователю будет показано сообщение о необходимости перезагрузки устройства. По ссылке **Изменить** можно изменить текст сообщения, а также период отображения сообщения и время выполнения автоматической перезагрузки.

     По умолчанию выбран этот вариант.

   - **Принудительно закрывать программы в заблокированных сеансах**

     Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства.

     По умолчанию параметр выключен.

2. В окне **Выбор учетных записей для доступа к устройствам** можно добавить учетные записи, которые будут использоваться для запуска задачи удаленной установки:

   - **Учетная запись не требуется (установлен Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (установка без Агента администрирования)**

Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя для установки программы.

Чтобы указать учетную запись пользователя, под которой будет запускаться программа установки, нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите учетные данные учетной записи пользователя.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

1. В окне **Запуск установки** нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

   Если в окне **Запуск установки** выбран параметр **Не запускать задачу после завершения работы мастера удаленной установки**, задача удаленной установки не будет запущена. Вы можете запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

► *Чтобы установить программу на устройства группы администрирования с помощью мастера удаленной установки:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области группы нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите пункт **Установить программу**.

   В результате запустится мастер удаленной установки. Следуйте далее указаниям мастера.
4. На последнем шаге мастера нажмите на кнопку **Далее** для создания и запуска задачи удаленной установки на выбранных устройствах.

После завершения работы мастера удаленной установки Kaspersky Security Center выполняет следующие действия:

- Создает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет размещается в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты** с именем, соответствующим названию и версии программы. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Сформированная задача удаленной установки размещается в папке **Задачи** или добавляется к задачам группы администрирования, для которой она была создана. Вы можете запустить эту задачу позже вручную. Имя задачи соответствует имени инсталляционного пакета для установки программы: **Установка <Имя инсталляционного пакета>**.

# Просмотр отчета о развертывании защиты

Для отслеживания процесса развертывания защиты в сети можно использовать отчет о развертывании защиты.

► *Чтобы просмотреть отчет о развертывании защиты:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В рабочей области закладки **Отчеты** выберите шаблон отчета **Отчет о развертывании защиты**.

В рабочей области будет сформирован отчет, содержащий информацию о развертывании защиты на всех устройствах сети.

Вы можете сформировать новый отчет о развертывании защиты и указать, информацию какого типа в него следует включать (см. стр. 583):

- для группы администрирования;
- для набора устройств;
- для выборки устройств;
- для всех устройств.

В рамках Kaspersky Security Center считается, что на устройстве развернута защита в том случае, когда на нем установлена программа безопасности и включена постоянная защита.

## Удаленная деинсталляция программ

Kaspersky Security Center позволяет удаленно деинсталлировать программы с устройств с помощью задач удаленной деинсталляции. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

### В этом разделе

### Удаленная деинсталляция программы с клиентских устройств группы администрирования

► *Чтобы удаленно деинсталлировать программу с клиентских устройств группы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находится нужная группа администрирования.
2. В дереве консоли выберите группу администрирования.
3. В рабочей области выберите закладку **Задачи**.
4. Запустите мастер создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана групповая задача удаленной деинсталляции выбранной программы. Созданная задача отображается в рабочей области группы администрирования, на закладке **Задачи**.
5. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с клиентских устройств группы администрирования.

### Удаленная деинсталляция программы с выбранных устройств

► *Чтобы удаленно деинсталлировать программу с выбранных устройств:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания задачи по кнопке **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

   В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Удаленная деинсталляция программы**.

   В результате работы мастера создания задачи будет создана задача удаленной деинсталляции выбранной программы для выбранного набора устройств. Созданная задача отображается в рабочей области папки **Задачи**.
3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной установки выбранная программа будет удалена с выбранных устройств.

## Работа с инсталляционными пакетами

При создании задач удаленной установки используются инсталляционные пакеты, которые содержат набор параметров, необходимых для установки программы.

Инсталляционные пакеты могут содержать в себе файл ключа. Не рекомендуется размещать в открытом доступе инсталляционные пакеты, содержащие в себе файл ключа.

Вы можете использовать один и тот же инсталляционный пакет многократно.

Сформированные для Сервера администрирования инсталляционные пакеты размещаются в дереве консоли в папке **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

## В этом разделе



## Создание инсталляционного пакета

► *Чтобы создать инсталляционный пакет:*

1. Подключитесь к нужному Серверу администрирования.
2. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
3. Запустите процесс создания инсталляционного пакета одним из следующих способов:
   - в контекстном меню папки **Инсталляционные пакеты** выберите пункт **Новый → Инсталляционный пакет**;
   - в контекстном меню списка инсталляционных пакетов выберите пункт **Создать → Инсталляционный пакет**;
   - по ссылке **Создать инсталляционный пакет** в блоке управления списком инсталляционных пакетов.

В результате запустится мастер создания инсталляционного пакета. Следуйте далее указаниям мастера.

В процессе создания инсталляционного пакета для программы "Лаборатории Касперского" вам может быть предложено ознакомиться с Лицензионным соглашением на эту программу и Политикой конфиденциальности программы. Внимательно прочитайте Лицензионное соглашение, которое заключается между вами и "Лабораторией Касперского", и Политику конфиденциальности. Если вы согласны со всеми пунктами Лицензионного соглашения и Политики конфиденциальности, в блоке **Я**

**подтверждаю, что полностью прочитал(а), понимаю и принимаю следующие положения и условия** установите флажки:

- **положения и условия настоящего Лицензионного соглашения;**
- **Политику конфиденциальности, которая описывает обработку данных.**

Установка программы будет продолжена после выбора обоих параметров. После этого создание инсталляционного пакета будет продолжено. Путь к файлу Лицензионного соглашения и Политики конфиденциальности задается в файле с расширением kud или kpd, входящем в состав дистрибутива программы, для которой создается инсталляционный пакет.

При создании инсталляционного пакета для программы Kaspersky Endpoint Security для Mac вы можете выбрать язык Лицензионного соглашения и Политики конфиденциальности.

Во время создания инсталляционного пакета для программы из базы программ "Лаборатории Касперского" вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), необходимых для установки этой программы. Мастер создания инсталляционного пакета отображает список всех возможных общесистемных компонентов для выбранной программы. Если инсталляционный пакет создается для патча (неполный дистрибутив), то в список общесистемных компонентов будут включены все необходимые для развертывания патча составляющие, вплоть до версии с полным дистрибутивом. Впоследствии вы можете ознакомиться с этим списком в свойствах инсталляционного пакета.

Для обновлений управляемых программ может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты** в дереве консоли.

Инсталляционный пакет для удаленной установки Агента администрирования не нужно создавать вручную. Он формируется автоматически при установке программы Kaspersky Security Center и располагается в папке **Инсталляционные пакеты**. Если пакет для удаленной установки Агента администрирования был удален, то для его повторного формирования в качестве файла с описанием следует выбрать файл nagent.kud, расположенный в папке NetAgent дистрибутива Kaspersky Security Center.

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

При создании инсталляционного пакета Сервера администрирования в качестве файла с описанием следует выбрать файл sc.kud, расположенный в корневой папке дистрибутива Kaspersky Security Center.

## См. также

Основной сценарий установки.....92

kaspersky

## Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки программ на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере, в общей папке или передать на клиентское устройство другим способом. Можно также отправить ссылку на автономный инсталляционный пакет по электронной почте. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center.

Убедитесь, что автономный инсталляционный пакет не доступен для неавторизованных лиц.

Вы можете создавать автономные инсталляционные пакеты как для программ "Лаборатории Касперского", так и для программ сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для программ сторонних производителей, необходимо сначала создать пользовательский инсталляционный пакет (см. стр. 375).

Источником для создания автономных инсталляционных пакетов являются инсталляционные пакеты в списке созданных на Сервере администрирования.

► *Чтобы создать автономный инсталляционный пакет:*

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите инсталляционный пакет, для которого требуется создать автономный пакет.

3. В контекстном меню выберите пункт **Создать автономный инсталляционный пакет**.

   В результате запускается мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На первой странице мастера, если вы выбрали инсталляционный пакет для программы "Лаборатории Касперского" и хотите установить Агент администрирования вместе с выбранной программой, убедитесь, что параметр **Установить Агент администрирования совместно с данной программой** включен.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

   Если автономный инсталляционный пакет для выбранной программы уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вы должны выбрать одно из следующих действий:

   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии программы, и чтобы также

остался автономный инсталляционный пакет для предыдущей версии программы, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.

- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этой же программы еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На следующей странице мастера выберите параметр **Переместить нераспределенные устройства в группу** и укажите группу администрирования, в которую вы хотите переместить устройства, после установки на них Агента администрирования.

   По умолчанию устройства перемещаются в группу **Управляемые устройства**.

   Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, выберите параметр **Не перемещать устройства**.

6. На следующей странице мастера, после завершения процесса создания автономного инсталляционного пакета, отобразится результат создания автономного инсталляционного пакета и путь к нему.

   Можно перейти по ссылкам и выполнить следующие действия:

   - Открыть папку с автономным инсталляционным пакетом.
   - Отправить по электронной почте ссылку на созданный автономный инсталляционный пакет. Для этого необходимо, чтобы была запущена программа для работы с электронной почтой.
   - Скопировать образец HTML-кода, чтобы разместить ссылку на веб-сайте. Текстовый файл (в формате TXT) создается и открывается с помощью программы, связанной с TXT-форматом. В файле отображается HTML-тег <a> с атрибутами.

7. Если вы хотите открыть список автономных инсталляционных пакетов, на следующей странице мастера включите параметр **Открыть список автономных пакетов**.

8. Нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку PkgInst общей папки Сервера администрирования (см. стр. 236). Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных инсталляционных пакетов**, расположенную над списком инсталляционных пакетов.

## Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любую программу (например, текстовый редактор) на клиентские устройства, например, с помощью задачи (см. стр. 1108);
- создать автономный инсталляционный пакет (см. стр. 374).

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Создавая пользовательский инсталляционный пакет, вы можете указать параметры командной строки, например, для установки программы в тихом режиме.

► *Чтобы создать пользовательский инсталляционный пакет:*

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Создать инсталляционный пакет** над списком инсталляционных пакетов.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На первой странице мастера выберите **Создать инсталляционный пакет из файла**.

4. На следующей странице мастера укажите имя пользовательского инсталляционного пакета.

5. На следующей странице мастера нажмите на кнопку **Обзор** и в стандартном окне **Открыть** выберите файл архива, расположенный на доступных дисках, чтобы создать пользовательский инсталляционный пакет.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать установочный пакет из файла формата SFX (самораспаковывающийся архив) нельзя.

   Файлы загружены с Сервера администрирования Kaspersky Security Center.

6. На следующей странице мастера укажите параметры командной строки для исполняемого файла.

   Вы можете указать параметры командной строки для установки программы из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   При необходимости настройте следующие параметры:

   - **Копировать всю папку в инсталляционный пакет**
   - **Конвертировать параметры на рекомендуемые значения для программ, распознаваемых Kaspersky Security Center**

   Начнется процесс создания пользовательского инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если пользовательский инсталляционный пакет не создан, отобразится соответствующее сообщение.

7. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования (см. стр. 236). После загрузки пользовательский инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов на Сервере администрирования можно просмотреть и изменить свойства пользовательского инсталляционного пакета (см. стр. 376).

## Просмотр и изменение свойств пользовательских инсталляционных пакетов

После создания пользовательского инсталляционного пакета в окне свойств можно просмотреть общую информацию о нем и указать параметры установки.

► *Чтобы просмотреть и изменить свойства пользовательского инсталляционного пакета:*

1. В дереве консоли выберите **Сервер администрирования** → **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В контекстном меню инсталляционного пакета выберите пункт **Свойства**.

   Откроется окно свойств выбранного инсталляционного пакета.

3. Отобразится следующая информация:
   - название инсталляционного пакета;
   - название программы, упакованной в пользовательский инсталляционные пакет;
   - версия программы;
   - дата создания инсталляционного пакета;
   - путь к пользовательскому инсталляционному пакету на Сервере администрирования;
   - параметры запуска исполняемого файла.
4. Задайте следующие параметры:
   - **Название инсталляционного пакета**
   - **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

     Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

     Если этот параметр выключен, необходимо установить пререквизиты вручную.

     По умолчанию параметр выключен.

     Этот параметр доступен, только если программа, добавленная в инсталляционный пакет, была распознана Kaspersky Security Center.

   - **Параметры запуска исполняемого файла**

     Если программе требуются дополнительные параметры для установки без вывода сообщений, укажите их в этом поле. Дополнительную информацию см. в документации производителя.

     Вы также можете указать и другие параметры.

     Эта параметр доступен только для пакетов, которые не были созданы на основе программ "Лаборатории Касперского".

5. Нажмите на кнопку **ОК** или **Применить**, чтобы сохранить изменения.

Новые параметры сохранены.

## См. также:

Создание пользовательского инсталляционного пакета .....375

kaspersky

## Получение инсталляционного пакета Агента администрирования из комплекта поставки Kaspersky Security Center

Вы можете получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center без необходимости установки Kaspersky Security Center. Затем вы можете использовать инсталляционный пакет для установки Агента администрирования на клиентские устройства.

► *Чтобы получить инсталляционный пакет Агента администрирования из комплекта поставки Kaspersky Security Center:*

1. Запустите исполняемый файл ksc_<номер версии>.<номер сборки>_full_<язык локализации> .exe из дистрибутива Kaspersky Security Center.
2. В появившемся окне перейдите по ссылке **Извлечь инсталляционные пакеты**.
3. В списке инсталляционных пакетов установите флажок рядом с инсталляционным пакетом Агента администрирования и нажмите на кнопку **Далее**.
4. При необходимости нажмите на кнопку **Обзор**, чтобы изменить отображаемую папку для извлечения инсталляционного пакета.
5. Нажмите на кнопку **Извлечь**.

   Программа извлекает инсталляционный пакет Агента администрирования.
6. После завершения процесса нажмите на кнопку **Закрыть**.

Инсталляционный пакет Агента администрирования распаковывается в выбранную папку.

С помощью инсталляционного пакета вы можете установить Агент администрирования одним из следующих способов:

- Локально (см. стр. 205) запустив файл setup.exe из извлеченной папки.
- С помощью автоматической установки (см. стр. 194)
- С помощью механизма групповых политик Microsoft Windows (см. стр. 184).

### См. также:



## Распространение инсталляционных пакетов на подчиненные Серверы администрирования

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Запустите создание задачи распространения инсталляционного пакета на подчиненные Серверы администрирования одним из следующих способов:

- Если вы хотите сформировать задачу для подчиненных Серверов выбранной группы администрирования, запустите создание групповой задачи для этой группы.
- Если вы хотите сформировать задачу для набора подчиненных Серверов, запустите создание задачи для набора устройств.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

В окне **Тип задачи** мастера создания задачи в узле **Сервер администрирования Kaspersky Security Center** в папке **Дополнительно** выберите тип задачи **Распространение инсталляционного пакета**.

В результате работы мастера создания задачи будет создана задача распространения выбранных инсталляционных пакетов на выбранные подчиненные Серверы администрирования.

3. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи выбранные инсталляционные пакеты будут скопированы на выбранные подчиненные Серверы администрирования.

## Распространение инсталляционных пакетов с помощью точек распространения

Для распространения инсталляционных пакетов в пределах группы администрирования вы можете использовать точки распространения.

После получения инсталляционных пакетов с Сервера администрирования точки распространения автоматически распространяют их на клиентские устройства с помощью многоадресной IP-рассылки. IP-рассылка новых инсталляционных пакетов в пределах группы администрирования производится один раз. Если в момент рассылки клиентское устройство было отключено от сети организации, то при запуске задачи установки Агент администрирования клиентского устройства автоматически скачивает необходимый инсталляционный пакет с точки распространения.

## Передача в Kaspersky Security Center информации о результатах установки программы

После создания инсталляционного пакета программы вы можете настроить инсталляционный пакет таким образом, чтобы диагностическая информация о результатах установки программы передавалась в Kaspersky Security Center. Для инсталляционных пакетов программ "Лаборатории Касперского" передача диагностической информации о результате установки программы настроена по умолчанию, дополнительная настройка не требуется.

► *Чтобы настроить передачу в Kaspersky Security Center диагностической информации о результате установки программы:*

1. Перейдите в папку инсталляционного пакета, сформированного средствами Kaspersky Security Center для выбранной программы. Эта папка расположена в папке общего доступа, которая была указана при установке Kaspersky Security Center.
2. Откройте файл с расширением kpd или kud для редактирования (например, с помощью текстового редактора "Блокнот" Microsoft Windows).

   Файл имеет формат обычного конфигурационного ini-файла.

3. Добавьте в файл следующие строки:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Эта команда настраивает программу Kaspersky Security Center таким образом, чтобы она ожидала окончания установки программы, для которой сформирован инсталляционный пакет и анализировала код возврата программы установки. Если нужно отключить передачу диагностической информации, установите для ключа Wait значение 0.

4. Внесите описание кодов возврата успешной установки. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_SuccessCodes]
   <код возврата>=[<описание>]
   <код возврата 1>=[<описание>]
   …
   ```

   В квадратных скобках приводятся необязательные ключи.

   Синтаксис строк:

   - `<код возврата>`. Любое число, соответствующее коду возврата программы установки. Количество кодов возврата может быть произвольным.
   - `<описание>`. Текстовое описание результата установки. Описание может отсутствовать.

5. Внесите описание кодов возврата для установки, завершенной с ошибкой. Для этого добавьте в файл следующие строки:

   ```
   [SetupProcessResult_ErrorCodes]
   <код возврата>=[<описание>]
   <код возврата 1>=[<описание>]
   …
   ```

   Синтаксис строк соответствует синтаксису строк кодов возврата при успешной установке.

6. Закройте kpd- или kud-файл, сохранив внесенные изменения.

Информация о результатах установки программы, указанной пользователем, будет записываться в журнал Kaspersky Security Center и отображаться в списке событий, в отчетах и в результатах выполнения задач.

## Определение адреса прокси-сервера KSN для инсталляционных пакетов

В случае изменения адреса или домена Сервера администрирования вы можете указать адрес прокси-сервера KSN для инсталляционного пакета.

► *Чтобы определить адрес прокси-сервера KSN для инсталляционного пакета:*

1. В дереве консоли в папке **Удаленная установка** двойным щелчком мыши нажмите на вложенную папку **Инсталляционные пакеты**.

2. В появившемся окне нажмите на кнопку **Свойства**.
3. В отобразившемся окне свойств выберите подраздел **Общие**.
4. В подразделе **Общие** окна свойств введите адрес прокси-сервера KSN.

Инсталляционные пакеты будут использовать этот адрес по умолчанию.

## Получение актуальных версий программ

В сертифицированной конфигурации не допускается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу из безопасного состояния.

Kaspersky Security Center позволяет получать актуальные версии корпоративных программ, хранящиеся на серверах "Лаборатории Касперского".

► *Чтобы получить актуальные версии корпоративных программ "Лаборатории Касперского":*

1. Выполните одно из следующих действий:
   - В дереве консоли выберите узел с именем нужного вам Сервера администрирования на закладке **Мониторинг** в разделе **Развертывание** перейдите по ссылке **Вышли новые версии программ "Лаборатории Касперского"**.

     Ссылка **Вышли новые версии программ "Лаборатории Касперского"** становится доступна, когда Сервер администрирования обнаруживает очередную версию корпоративной программы на интернет-сервере "Лаборатории Касперского".

   - В дереве консоли выберите **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**, в рабочей области нажмите **Дополнительные действия** и в раскрывающемся списке выберите пункт **Посмотреть текущую версию Программы "Лаборатории Касперского"**.

   Появится список текущих версий программ "Лаборатории Касперского".
2. Можно отфильтровать список программ "Лаборатории Касперского", чтобы упростить поиск нужной программы.

   В верхней части окна **Текущие версии программ** перейдите по ссылке **Фильтровать** для фильтрации списка программ по следующим критериям:

   - **Компоненты**. Используйте этот критерий, чтобы отфильтровать список программ "Лаборатории Касперского" по областям защиты, которые используются в вашей сети.
   - **Тип ПО для загрузки**. Используйте этот критерий, чтобы отфильтровать список программ "Лаборатории Касперского" по типу программы.
   - **Какие обновления и ПО показывать**. Используйте этот критерий, чтобы отобразить доступные программы "Лаборатории Касперского" по определенным версиям.
   - **На каких языках показывать ПО и обновления**. Используйте этот критерий для отображения программ "Лаборатории Касперского" с определенным языком локализации.

   Нажмите на кнопку **Применить**, чтобы применить изменения.
3. Выберите в списке нужную вам программу.

4. Загрузите дистрибутив программы по ссылке в строке **Веб-адрес дистрибутива**.

> Для обновлений управляемых программ может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

Если для выбранной программы отображается кнопка **Загрузить программы и создать инсталляционные пакеты**, вы можете нажать на эту кнопку для загрузки дистрибутива программы и автоматического создания инсталляционного пакета. В этом случае Kaspersky Security Center загружает дистрибутив программы на Сервер администрирования в папку общего доступа, заданную при установке Kaspersky Security Center. Список автоматически созданных инсталляционных пакетов отображается в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

> После закрытия окна **Актуальные версии программ** ссылка **Вышли новые версии программ "Лаборатории Касперского"** исчезает из блока **Развертывание**.

Вы можете создавать инсталляционные пакеты новых версий программ и работать с созданными инсталляционными пакетами в папке **Удаленная установка** дерева консоли, во вложенной папке **Инсталляционные пакеты**.

Вы также можете открыть окно **Актуальные версии программ** по ссылке **Просмотреть актуальные версии программ "Лаборатории Касперского"** в рабочей области папки **Инсталляционные пакеты**.

## См. также:

kaspersky

# Подготовка Windows-устройства к удаленной установке. Утилита riprep

Удаленная установка программы на клиентском устройстве может завершаться с ошибкой по следующим причинам:

- Задача ранее уже была успешно выполнена на этом устройстве. В этом случае ее повторное выполнение не требуется.
- Во время запуска задачи устройство было выключено. В этом случае требуется включить устройство и запустить задачу еще раз.
- Отсутствует связь между Сервером администрирования и Агентом администрирования, установленным на клиентском устройстве. Для определения причины проблемы вы можете воспользоваться утилитой удаленной диагностики клиентского устройства (klactgui).
- Если на устройстве не установлен Агент администрирования, при удаленной установке программы могут возникнуть следующие проблемы:
  - на клиентском устройстве включен параметр **Простой общий доступ к файлам**;
  - на клиентском устройстве не работает служба Server;
  - на клиентском устройстве закрыты необходимые порты;
  - у учетной записи, под которой выполняется задача, недостаточно прав.

  Для решения проблем, возникших при установке программы на клиентское устройство, на котором не установлен Агент администрирования, вы можете воспользоваться утилитой подготовки устройства к удаленной установке (riprep).

В этом разделе описывается утилита подготовки устройства к удаленной установке (riprep). Она расположена в папке установки Kaspersky Security Center на устройстве с установленным Сервером администрирования.

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

## В этом разделе



## Подготовка Windows-устройства к удаленной установке в интерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в интерактивном режиме:*

1. На клиентском устройстве запустите файл riprep.exe.
2. В открывшемся главном окне утилиты подготовки к удаленной установке выберите следующие параметры:
   - **Отключить простой общий доступ к файлам.**
   - **Запустить службу Сервера администрирования.**
   - **Открыть порты.**

- **Добавить учетную запись.**
- **Отключить контроль учетных записей** (параметр доступен для операционных систем Microsoft Windows Vista, Microsoft Windows 7 и Microsoft Windows Server 2008).

3. Нажмите на кнопку **Запустить**.

В результате в нижней части главного окна утилиты отображаются этапы подготовки устройства к удаленной установке.

Если вы выбрали параметр **Добавить учетную запись**, при создании учетной записи будет выведен запрос на ввод имени учетной записи и пароля. В результате будет создана локальная учетная запись, принадлежащая группе локальных администраторов.

Если вы выбрали параметр **Отключить контроль учетных записей**, попытка отключения контроля учетных записей будет выполняться и в том случае, когда до запуска утилиты контроль учетных записей был отключен. После отключения контроля учетных записей будет выведен запрос на перезагрузку устройства.

## Подготовка устройства к удаленной установке в неинтерактивном режиме

► *Чтобы подготовить устройство к удаленной установке в неинтерактивном режиме:*

на клиентском устройстве запустите файл riprep.exe из командной строки с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Описания ключей:

- `-silent` – запуск утилиты в неинтерактивном режиме.
- `-cfg CONFIG_FILE` – определение конфигурации утилиты, где `CONFIG_FILE` – путь к файлу конфигурации (файл с расширением .ini).
- `-tl traceLevel` – задание уровня трассировки, где `traceLevel` – число от 0 до 5. Если ключ не задан, то используется значение 0.

В результате запуска утилиты в неинтерактивном режиме вы можете выполнить следующие задачи:

- отключение простого общего доступа к файлам;
- запуск службы Server на клиентском устройстве;
- открытие портов;
- создание локальной учетной записи;
- отключение контроля учетных записей (UAC).

Вы можете задать параметры подготовки устройства к удаленной установке в конфигурационном файле, указанном в ключе `-cfg`. Чтобы задать эти параметры, в конфигурационный файл нужно добавить следующую информацию:

- В разделе `Common` указать, какие задачи следует выполнять:
  - `DisableSFS` – отключение простого общего доступа к файлам (0 – задача выключена; 1 – задача включена).
  - `StartServer` – запуск службы Server (0 – задача выключена; 1 – задача включена).

- `OpenFirewallPorts` – открытие необходимых портов (0 – задача выключена; 1 – задача включена).
- `DisableUAC` – отключение контроля учетных записей (0 – задача выключена; 1 – задача включена).
- `RebootType` – определение поведения при необходимости перезагрузки при отключенном контроле учетных записей (UAC). Вы можете использовать следующие значения параметра:
  - 0 – никогда не перезагружать устройство;
  - 1 – перезагружать устройство, если до запуска утилиты контроль учетных записей был включен;
  - 2 – перезагружать устройство принудительно, если до запуска утилиты контроль учетных записей был включен;
  - 4 – всегда перезагружать устройство;
  - 5 – всегда принудительно перезагружать устройство.

- В разделе `UserAccount` указать имя учетной записи (`user`) и ее пароль (`Pwd`).

Пример содержимого конфигурационного файла:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

По окончании работы утилиты в папке запуска создаются следующие файлы:

- riprep.txt – отчет о работе, в котором перечислены этапы работы утилиты с причинами их проведения;
- riprep.log – файл трассировки (создается, если заданный уровень трассировки больше 0).

## Подготовка устройства с операционной системой Linux к удаленной установке Агента администрирования

► *Чтобы подготовить устройство с операционной системой Linux к удаленной установке Агента администрирования:*

1. Убедитесь, что на целевом устройстве с операционной системой Linux установлено следующее программное обеспечение:
   - Sudo
   - Интерпретатор языка Perl версии 5.10 или выше.
2. Выполните проверку конфигурации устройства:
   a. Проверьте, что возможно подключение к устройству через SSH (например, программа PuTTY).

      Если вы не можете подключиться к устройству, откройте файл /etc/ssh/sshd_config и убедитесь, что следующие параметры имеют значения:

```
PasswordAuthentication no
ChallengeResponseAuthentication yes
```

Не изменяйте файл /etc/ssh/sshd_config, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

a. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

b. Используйте команду sudo `visudo`, чтобы открыть конфигурационный файл sudoers.

В открывшемся файле найдите строку, начинающуюся с `%sudo` (или с `%wheel` если вы используете операционную систему CentOS). Под этой строкой укажите следующее: `<username> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<username>` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH. Если вы используете операционную систему Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`.

c. Сохраните и закройте файл sudoers.

d. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

1. Откройте файл /etc/systemd/logind.conf и выполните одно из следующих действий:

   - Укажите значение 'no' для параметра KillUserProcesses: `KillUserProcesses=no`.
   - Для параметра KillExcludeUsers введите имя пользователя учетной записи, под которой будет выполняться удаленная установка, например, `KillExcludeUsers=root`.

   Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

2. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 387) и настройте Агент администрирования.

3. Загрузите и создайте инсталляционный пакет:

   a. Перед установкой пакета на устройство убедитесь, что на нем установлены зависимости (программы, библиотеки) для данного пакета.

   Вы можете самостоятельно посмотреть зависимости для каждого пакета, используя утилиты, специфичные для того дистрибутива Linux, на который будет устанавливаться пакет. С информацией об утилитах вы можете ознакомиться в документации к вашей операционной системе.

   b. Загрузите инсталляционный пакет Агент администрирования.

   c. Для создания пакета удаленной установки используйте файлы:

      - klnagent.kpd;

- akinstall.sh;
- deb или rpm пакет Агента администрирования.

4. Создайте задачу удаленной установки программы с параметрами:
   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
   - В окне **Выбор учетной записи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.
5. Запустите задачу удаленной установки программы. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка может завершиться ошибкой, если вы устанавливаете Агент администрирования с использованием протокола SSH на устройства с операционными системами Fedora версии ниже 20. В этом случае для успешной установки Агента администрирования в файле /etc/sudoers закомментируйте параметр Defaults requiretty (заключите его в синтаксис комментария, чтобы удалить его из проанализированного кода). Подробное описание того, почему параметр Defaults requiretty может вызвать проблемы при подключении по SSH, вы можете найти на сайте системы отслеживания проблем Bugzilla (https://bugzilla.redhat.com/show_bug.cgi?id=1020147).

## Подготовка устройства под управлением SUSE Linux Enterprise Server 15 к установке Агента администрирования

► *Чтобы установить Агент администрирования на устройство с операционной системой SUSE Linux Enterprise Server 15,*

перед установкой Агента администрирования выполните следующую команду:

```
$ sudo zypper install insserv-compat
```

Это позволит вам установить пакет insserv-compat и правильно настроить Агент администрирования.

Выполните команду `rpm -q insserv-compat`, чтобы проверить, если пакет уже установлен.

Если в вашей сети много устройств под управлением SUSE Linux Enterprise Server 15, вы можете использовать специальное программное обеспечение для настройки и управления инфраструктурой компании. Используя это программное обеспечение, вы можете автоматически установить пакет insserv-compat сразу на все необходимые устройства. Например, вы можете использовать Puppet, Ansible, Chef, или сделать свой скрипт любым удобным для вас способом.

Помимо установки пакета insserv-compat, убедитесь, что ваши Linux-устройства полностью подготовлены (см. стр. 385). После этого разверните и установите Агент администрирования (см. стр. 1035).

kaspersky

# Подготовка устройства с операционной системой macOS к удаленной установке Агента администрирования

► *Чтобы подготовить устройство с операционной системой macOS к удаленной установке Агента администрирования:*

1. Убедитесь, что на целевом устройстве с операционной системой macOS установлена программа sudo.
2. Выполните проверку конфигурации устройства:
   a. Убедитесь, что открыт порт 22 на клиентском устройстве. Для этого в разделе **Системные настройки** откройте панель **Обмен** и убедитесь, что установлен флажок **Удаленный вход**.

      Вы можете подключиться к клиентскому устройству по протоколу Secure Shell (SSH) только через порт 22. Вы не можете изменить номер порта.

      Вы можете использовать команду `ssh <имя_устройства>` для удаленного входа на устройство macOS. На панели **Общий доступ** можно использовать параметр **Разрешить доступ для** чтобы задать область действия пользователей, которым разрешен доступ к устройству macOS.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

      Используйте команду `sudo visudo`, чтобы открыть конфигурационный файл sudoers в терминале. В файле, который вы открыли, в поле `Спецификация привилегий пользователя` укажите следующее: `username ALL = (ALL) NOPASSWD: ALL`. В этом случае `username` является учетной записью пользователя, которая будет использоваться для подключения к устройству по протоколу SSH.

   c. Сохраните и закройте файл sudoers.

   d. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

3. Загрузите и создайте инсталляционный пакет:
   a. Загрузите инсталляционный пакет Агента администрирования одним из следующих способов:
      - В дереве консоли, в контекстном меню выбрав **Удаленная установка** → **Инсталляционные пакеты** и далее **Показать текущие версии программ**, чтобы выбрать из доступных пакетов.
      - Загрузив соответствующую версию Агента администрирования с веб-сайта Службы технической поддержки по адресу https://support.kaspersky.ru/ https://support.kaspersky.ru
      - Запросив инсталляционный пакет у специалистов Службы технической поддержки.

   b. Для создания пакета удаленной установки используйте файлы:
      - klnagent.kud;
      - install.sh;
      - klnagentmac.dmg.

4. Создайте задачу удаленной установки программы с параметрами:
    - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
    - В окне **Выбор учетной записи для запуска задачи** для запуска задачи укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

Клиентское устройство готово к удаленной установке Агента администрирования с помощью соответствующей задачи, которую вы создали.

# Программы "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых программ "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации программа формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

## См. также:



## В этом разделе

kaspersky

# Лицензирование управляемых программ

Программы "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждой из программ. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемой программы;
- с помощью задачи *Добавление лицензионного ключа* управляемой программы;
- с помощью активации управляемой программы вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Программа "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Программа, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

**Автоматическое распространение**

Если вы используете разные управляемые программы и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Программа определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае нельзя предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение (см. стр. 341), таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 393).
  - Автоматическое распространение лицензионного ключа (на стр. 395).

  Или

- Kaspersky Security Center 14.2 Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 1068).
  - Автоматическое распространение лицензионного ключа (на стр. 1069).

**Добавление файла ключа или кода активации в инсталляционный пакет управляемой программы.**

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этой программы. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
  - Создание инсталляционного пакета (на стр. 372).
  - Установка программ на клиентские устройства (на стр. 810).

  Или
- Kaspersky Security Center 14.2 Web Console: Добавление лицензионного ключа в инсталляционный пакет (см. стр. 1029).

**Распространение с помощью задачи добавления лицензионного ключа управляемой программы**

В случае использования задачи *Добавление лицензионного ключа* управляемой программы вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 393).
  - Распространение лицензионного ключа на клиентские устройства (на стр. 395).

  Или
- Kaspersky Security Center 14.2 Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 1068).
  - Распространение лицензионного ключа на клиентские устройства (на стр. 1068).

**Добавление кода активации или файла ключа вручную на устройства.**

Вы можете активировать установленную программу "Лаборатории Касперского" локально, используя инструменты программы. Дополнительную информацию см. в документации к установленным программам.

kaspersky

## См. также



# Просмотр информации об используемых лицензионных ключах

► *Чтобы просмотреть информацию об используемых лицензионных ключах,*

В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.

В рабочей области папки отображается перечень лицензионных ключей, используемых на клиентских устройствах.

Рядом с каждым лицензионным ключом отображается значок, соответствующий типу его использования:

-  – информация об используемом лицензионном ключе получена от подключенного к Серверу администрирования клиентского устройства. Файл этого лицензионного ключа не хранится на Сервере администрирования.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Автоматическое распространение этого лицензионного ключа отключено.
-  – лицензионный ключ находится в хранилище Сервера администрирования. Включено автоматическое распространение этого лицензионного ключа.

Вы можете просмотреть информацию о том, какие лицензионные ключи используются для активации программы на клиентском устройстве, в разделе **Программы** окна свойств клиентского устройства (см. стр. 448).

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871).

kaspersky

## См. также



# Добавление лицензионного ключа в хранилище Сервера администрирования

► *Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:*

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. Запустите задачу добавления лицензионного ключа одним из следующих способов:
   - В контекстном меню списка лицензионных ключей выберите пункт **Добавить код активации или файл ключа**.
   - Перейдите по ссылке **Добавить код активации или файл ключа** в блоке управления списком лицензионных ключей.
   - Нажмите на кнопку **Добавить код активации или файл ключ**.

   Запустится мастер добавления лицензионного ключа.
3. Выберите способ активации Сервера администрирования: с помощью кода активации или с помощью файла ключа.
4. Укажите ваш код активации или файл ключа.
5. Выберите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**, если вы хотите распространить соответствующий лицензионный ключ в своей сети немедленно. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ (см. стр. 395).

В результате файл ключа загружается и мастер добавления лицензионного ключа завершается. Теперь вы можете увидеть этот лицензионный ключ в списке лицензий "Лаборатории Касперского".

### См. также



## Удаление лицензионного ключа Сервера администрирования

► *Чтобы удалить лицензионный ключ Сервера администрирования:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.
3. Удалите лицензионный ключ по кнопке **Удалить**.

Лицензионный ключ будет удален.

Если был добавлен резервный лицензионный ключ, он автоматически становится активным после удаления предыдущего активного лицензионного ключа.

После удаления активного лицензионного ключа для Сервера администрирования становятся недоступными функции Системное администрирование (см. стр. 353) и Управление мобильными устройствами (см. стр. 353). Можно добавить (см. стр. 393) удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

### См. также

kaspersky

## Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи распространения лицензионного ключа.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования (см. стр. 393).

► *Чтобы распространить лицензионный ключ на клиентские устройства:*

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Распространить ключ на управляемые устройства** в блоке управления списком лицензионных ключей.

Запустится мастер создания задачи активации программы. Следуйте далее указаниям мастера.

Задачи, сформированные при помощи мастера создания задачи активации программы, являются задачами для наборов устройств и размещаются в папке **Задачи** дерева консоли.

Вы также можете создать групповую или локальную задачу распространения лицензионного ключа с помощью мастера создания задачи для группы администрирования и для клиентского устройства.

### См. также



## Автоматическое распространение лицензионного ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства:*

1. В дереве консоли выберите папку **Лицензии "Лаборатории Касперского"**.
2. В рабочей области папки выберите лицензионный ключ, который вы хотите автоматически распространять на устройства.

3. Откройте окно свойств выбранного лицензионного ключа одним из следующих способов:
   - в контекстном меню лицензионного ключа выберите пункт **Свойства**;
   - по ссылке **Посмотреть свойства ключа** в блоке работы с выбранным лицензионным ключом.
4. В открывшемся окне свойств лицензионного ключа установите флажок **Распространить лицензионный ключ на управляемые устройства**. Закройте окно свойств лицензионного ключа.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для программы при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. (Лицензионное ограничение задано в свойствах лицензионного ключа.) Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Если вы установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**, соответствующий лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ (см. стр. 395).

### См. также:



## Создание и просмотр отчета об использовании лицензионных ключей

► *Чтобы создать отчет об использовании лицензионных ключей на клиентских устройствах:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите шаблон отчета **Отчет об использовании лицензионных ключей** или создайте новый шаблон отчета одноименного типа.

В результате в рабочей области отчета об использовании лицензионных ключей отображается информация об активных и резервных лицензионных ключах, используемых на клиентских устройствах. Также в отчете содержатся сведения об устройствах, на которых используются лицензионные ключи, и об ограничениях, заданных в свойствах лицензионных ключей.

### См. также



## Просмотр информации о лицензионных ключах программы

► *Чтобы узнать, какие лицензионные ключи используются программой "Лаборатории Касперского":*

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на закладку **Устройства**.
2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Программы**.
4. В появившемся списке программ выберите программу, лицензионные ключи которой вы хотите просмотреть, и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств Сервера администрирования выберите раздел **Лицензионные ключи**.

   Информация отображается в рабочей области этого раздела.

# Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

### В этом разделе

kaspersky

## Безопасное состояние

Программа находится в безопасном состоянии (сертифицированной конфигурации), если выполняются следующие условия:

- Параметры программы находятся в рамках допустимых значений, приведенных в приложении к этому документу.

## Проверка работоспособности Kaspersky Security Center

После установки Kaspersky Security Center вы можете проверить его работоспособность с помощью выполнения алгоритма проверки. В таблице ниже приведен порядок действий для проверки работоспособности программы и ожидаемые результаты выполнения этих действий.

*Таблица 55. Шаги алгоритма проверки работоспособности Kaspersky Security Center*

| Номер шага | Действие | Результат |
|---|---|---|
| 1 | Подключитесь к Серверу администрирования с помощью Консоли Администрирования (см. стр. 300). | Консоль администрирования подключена к Серверу администрирования. В списке управляемых устройств появилось как минимум одно устройство Сервера администрирования. |
| 2 | Выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки (см. стр. 285). | Мастер первоначальной настройки создал необходимые для развертывания защиты политики и задачи с параметрами по умолчанию. |
| 3 | Установите Агент администрирования и Kaspersky Endpoint Security для Windows на устройство (см. стр. 359). | Управляемое устройство, на которое была произведена установка программ, присутствует в списке нераспределенных устройств.<br>В свойствах устройства в разделе **Программы** присутствуют программы Агент администрирования и Kaspersky Endpoint Security для Windows. |
| 4 | Загрузите обновления в хранилище Сервера администрирования, запустив задачу загрузки обновлений в хранилище (см. стр. 461). Подробнее см. в Руководстве по эксплуатации, в разделе "Создание задачи загрузки обновлений в хранилище". | Задача завершена успешно и обновления загружены в хранилище. |

| Номер шага | Действие | Результат |
|---|---|---|
| 5 | Обновите программу безопасности Kaspersky Endpoint Security для Windows. Для этого выполните задачу обновления (см. стр. 473). Подробнее см. в Руководстве по эксплуатации, в разделе "Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства". | В свойствах управляемого устройства в разделе **Программы** в свойствах программы Kaspersky Endpoint Security для Windows дата последнего обновления баз соответствует дате последнего запуска задачи обновления. |
| 6 | Внесите произвольные тестовые изменения в политику Kaspersky Endpoint Security для Windows. | Политика применена на управляемом устройстве, обнаруженном в сети:<br>• В свойствах политики присутствует информация о том, что она применена на устройства (см. стр. 567).<br>• Параметры программы безопасности соответствуют параметрам политики. |
| 7 | Скопируйте на одно из управляемых устройств тестовый файл EICAR (см. стр. 320). | В журнале событий есть записи об обнаружении и ликвидации зараженного файла. В свойствах устройства в разделе **Защита** в поле **Обнаружено вирусов** значение увеличилось на один. |

kaspersky

# Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

## В этом разделе



## См. также:


Настройка и распространение политик: подход, ориентированный на устройства ..... 402
Настройка и распространение политик: подход, ориентированный на пользователя ..... 1081


# Сценарий: Настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

**Предварительные требования**

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center (см. стр. 238).
- Установили Kaspersky Security Center 14.2 Web Console (см. стр. 950) (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center (см. стр. 92).
- Мастер первоначальной настройки (см. стр. 1007) завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования;
  - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

**a. Настройка и распространение политик и профилей политик для программ "Лаборатории Касперского"**

Для настройки и распространения параметров программ "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью (см. стр. 404): ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства (см. стр. 402) метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center 14.2 Web Console. Для реализации ориентированного на пользователей (см. стр. 1081) метода управления безопасностью подходит только Kaspersky Security Center 14.2 Web Console.

**b. Настройка задач для удаленного управления программами "Лаборатории Касперского"**

Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

Инструкции:

Консоль администрирования:

Настройка групповой задачи обновления Kaspersky Endpoint Security (см. стр. 408).

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).

Kaspersky Security Center 14.2 Web Console:

Настройка групповой задачи обновления Kaspersky Endpoint Security (см. стр. 1104).

Параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

При необходимости создайте дополнительные задачи (см. стр. 411) управления программами "Лаборатории Касперского", установленными на клиентских устройствах.

**c. Оценка и ограничение загрузки событий в базу данных**

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

Консоль администрирования: Настройка количества событий в хранилище событий (см. стр. 410).

Kaspersky Security Center 14.2 Web Console: Настройка количества событий в хранилище событий (см. стр. 983).

kaspersky

**Результаты**

После завершения этого сценария ваша сеть будет защищена благодаря настройке программ "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Программы "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление программами осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и программ "Лаборатории Касперского" (см. стр. 449).

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в онлайн-справке Kaspersky Sandbox 2.0 https://support.kaspersky.com/KSB/2.0/ru-RU/189425.htm.

## См. также:



# Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

**Предварительные требования**

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center (см. стр. 238) и Kaspersky Security Center 14.2 Web Console (см. стр. 950) (если требуется). Если вы установили Kaspersky Security Center 14.2 Web Console, вам может быть интересно также управление безопасностью (см. стр. 1081), ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

**Этапы**

Сценарий управления программами "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

**a. Настройка политик программ**

Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. стр. 1174) для каждой программы. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих программ:

Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.

Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux.

Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. стр. 405).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их в вышележащей политике. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. 426) позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

Консоль администрирования: Создание политики (см. стр. 430).

Kaspersky Security Center 14.2 Web Console: Создание политики (см. стр. 1174).

**b. Создание профилей политики (если требуется)**

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики (см. стр. 1171) для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги (см. стр. 1159). Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные программы "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

Консоль администрирования:

Создание профиля политики (см. стр. 439).

Создание правила активации профиля политики (см. стр. 441).

Kaspersky Security Center 14.2 Web Console:

Создание профиля политики (см. стр. 1184).

Создание правила активации профиля политики (см. стр. 1186).

**c. Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно (см. стр. 726). Также синхронизация выполняется принудительно после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center 14.2 Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

Консоль администрирования: Принудительная синхронизация (см. стр. 726).

Kaspersky Security Center 14.2 Web Console: Принудительная синхронизация (см. стр. 1272).

**Результаты**

После завершения сценария, ориентированного на устройства, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики программ и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

### См. также:



## Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры программ к разным устройствам, вы можете использовать один или оба типа управления в комбинации. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center 14.2 Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center 14.2 Web Console.

Управление безопасностью, ориентированное на устройства (см. стр. 402), позволяет вам применять различные параметры программы безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

Управление безопасностью, ориентированное на пользователя (см. стр. 1081), позволяет вам применять различные параметры программ безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры программы для устройств, принадлежащих

пользователям с различными ролями. Например, можно применить различные параметры программ к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с программами "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры программы могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры программ для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать инциденты безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры программы. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики (см. стр. 83) для каждой группы администрирования, а затем дополнительно создать профили политик (см. стр. 85) для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей (см. стр. 1224).

### См. также:

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Сценарий: Настройка защиты сети .....400

## Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки (см. стр. 285). Вы можете выполнить настройку в окне свойств политики.

При изменении параметра следует помнить, что для того, чтобы значение параметра использовалось на рабочей станции, следует нажать на кнопку с "замком" над параметром.

### См. также:

Настройка и распространение политик: Убедитесь, что открыт порт 22 на клиентском устройстве402

### В этом разделе

kaspersky

## Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Продвинутая защита** можно настроить использование Kaspersky Security Network для Kaspersky Endpoint Security для Windows. Можно также настроить модули Kaspersky Endpoint Security для Windows, такие как Анализ поведения, Защита от эксплойтов, Предотвращение вторжений и Откат вредоносных действий.

В подразделе **Kaspersky Security Network** рекомендуется включить параметр **Использовать прокси-сервер KSN**. Использование этого параметра поможет перераспределить и оптимизировать трафик сети. Если параметр **Использовать KSN-прокси** выключен, вы можете включить прямое использование серверов KSN (см. стр. 829).

### См. также:

Сценарий: Настройка защиты сети .....400

## Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Необходимая защита от угроз** окна свойств политики, рекомендуется указать дополнительные параметры в подразделах **Сетевой экран** и **Защита от файловых угроз**.

Подраздел **Сетевой экран** содержит параметры, позволяющие контролировать сетевую активность программ на клиентских устройствах. Клиентское устройство использует сеть, которой присвоен один из следующих статусов: общедоступная, локальная или доверенная. В зависимости от состояния сети Kaspersky Endpoint Security может разрешить или запретить сетевую активность на устройстве. Когда вы добавляете новую сеть в свою организацию, вы должны присвоить ей соответствующий сетевой статус. Например, если клиентским устройством является ноутбук, рекомендуется, чтобы это устройство использовало общедоступную или доверенную сеть, так как ноутбук не всегда подключен к локальной сети. В подразделе **Сетевой экран** можно проверить, правильно ли присвоены статусы используемым в вашей организации сетям.

► *Чтобы проверить список сетей:*

1. В свойствах политики перейдите в раздел **Базовая защита** → **Сетевой экран**.
2. В блоке **Доступные сети** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Сетевой экран** перейдите на закладку **Сети** для просмотра списка сетей.

В подразделе **Защита от файловых угроз** можно отключить проверку сетевых дисков. Проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

► *Чтобы выключить проверку сетевых дисков:*

1. В свойствах политики перейдите в раздел **Параметры программы** → **Базовая защита** → **Защита от файловых угроз**.
2. В блоке **Уровень безопасности** нажмите на кнопку **Настройка**.
3. В открывшемся окне **Защита от файловых угроз** на закладке **Общие** снимите флажок **Все сетевые диски**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка политики в разделе Дополнительные параметры

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Общие параметры** окна свойств политики, рекомендуется указать дополнительные параметры, а также а подразделах **Отчеты и хранилища** и **Интерфейс**.

В подразделе **Отчеты и хранилища**, перейдите в раздел **Передача данных на Сервер администрирования**. Флажок **О запускаемых программах** – если флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Если флажок установлен, сохраненная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов). Снимите флажок **О запускаемых программах**, если он установлен в политике верхнего уровня.

Если Консоль администрирования управляет антивирусной защитой в сети организации централизованно, отключите отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях. Для этого в подразделе **Интерфейс** перейдите в раздел **Взаимодействие с пользователем** и выберите параметр **Не отображать**.

Чтобы включить защиту паролем на рабочих станциях, в подразделе **Интерфейс** перейдите в раздел **Защита паролем**, нажмите на кнопку **Параметры** и установите флажок **Включить защиту паролем**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка политики в разделе Настройка событий

В разделе **Настройка событий** следует отключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На закладке **Критическое событие**:
  - Автозапуск программы выключен.
  - Доступ запрещен.
  - Запуск программы запрещен.

- Лечение невозможно.
- Нарушено Лицензионное соглашение.
- Не удалось загрузить модуль шифрования.
- Невозможен запуск двух задач одновременно.
- Обнаружена активная угроза. Требуется запуск процедуры лечения.
- Обнаружена сетевая атака.
- Обновлены не все компоненты.
- Ошибка активации.
- Ошибка активации портативного режима.
- Ошибка взаимодействия с Kaspersky Security Center.
- Ошибка деактивации портативного режима.
- Ошибка изменения состава программы.
- Ошибка применения правил шифрования / расшифровки файлов.
- Политика не может быть применена.
- Процесс завершен.
- Сетевая активность запрещена.

- На закладке **Отказ функционирования**:
  - Ошибка в параметрах задачи. Параметры задачи не применены.
- На закладке **Предупреждение**:
  - Самозащита программы выключена.
  - Некорректный резервный код активации.
  - Пользователь отказался от политики шифрования.
- На закладке **Информационное сообщение**:
  - Запуск программы запрещен в тестовом режиме.

## Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальным и рекомендуемым расписанием для Kaspersky Endpoint Security версии 10 и выше является **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. По умолчанию для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**.

Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. Следует настроить оптимальное расписание этой задачи исходя из принятого в организации регламента работы.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка расписания задачи Поиск уязвимостей и требуемых обновлений

Мастер первоначальной настройки создает для Агента администрирования групповую задачу *Поиск уязвимостей и требуемых обновлений*. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий: Настройка защиты сети ..... 400

## Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, параметр **Запускать пропущенные задачи** выключен.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программы вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые. Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

► *Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:*

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **ОК**.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

См. также:

Сценарий: Мониторинг и отчеты ..... 576

Сценарий: Настройка защиты сети ..... 400

## Установка максимального срока хранения информации о закрытых уязвимостях

Чтобы установить максимальный срок хранения в базе данных информации об уже закрытых уязвимостях на управляемых устройствах:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. В разделе **Хранилище событий** укажите максимальный срок хранения информации о закрытых уязвимостях в базе данных.

   Срок, заданный по умолчанию, – 90 дней.

3. Нажмите на кнопку **ОК**.

Максимальный срок хранения информации о закрытых уязвимостях ограничен указанным количеством дней. После этого задача обслуживания Сервера администрирования удалит устаревшую информацию из базы данных.

## Управление задачами

Kaspersky Security Center управляет работой программ, установленных на устройствах, путем создания и запуска различных задач. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Задачи делятся на следующие типы:

- *Групповые задачи*. Задачи, которые выполняются на устройствах выбранной группы администрирования.
- *Задачи Сервера администрирования*. Задачи, которые выполняются на Сервере администрирования.
- *Задачи для наборов устройств*. Глобальные задачи – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.
- *Локальные задачи*. Локальные задачи – это задачи, которые выполняются на конкретном устройстве.

Создание задач для программы возможно только в случае, если на рабочее место администратора установлен плагин управления этой программой.

Список устройств, для которых будет создана задача, можно сформировать одним из следующих способов:

- Выбрать устройства, обнаруженные в сети Сервером администрирования.
- Задать список устройств вручную. В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.
- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

  Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования при подключении устройств или в результате обнаружения устройств.

Для каждой программы вы можете создавать любое количество групповых задач, задач для наборов устройств и локальных задач.

Обмен информацией о задачах между программой, установленной на устройстве, и информационной базой Kaspersky Security Center происходит в момент соединения Агента администрирования с Сервером администрирования.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи. При остановке программы выполнение всех запущенных задач прекращается.

Результаты выполнения задач сохраняются в журналах событий Microsoft Windows и в Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

**Управление задачами для программ, поддерживающих мультитенантность**

Групповая задача для мультитенантных программ применяется к программам в зависимости от иерархии Серверов администрирования и клиентских устройств. Виртуальный Сервер администрирования, на котором создана задача, должен быть в той же группе администрирования, что и клиентское устройство, на котором установлена программа, или в группе более низкого уровня.

В событиях, которые соответствуют результатам выполнения задачи, администратору поставщика услуг отображается информация об устройстве, на котором выполнена задача. В свою очередь, тенанту отображается **Мультитенантный узел**.

kaspersky

## См. также:



## В этом разделе



## Создание задачи

В Консоли администрирования можно создавать задачи непосредственно в папке группы администрирования, для которой создается задача, и в рабочей области папки **Задачи**.

► *Чтобы создать задачу в папке группы администрирования:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать задачу.
2. В рабочей области выберите закладку **Задачи**.
3. Запустите мастер создания задачи по кнопке **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

► *Чтобы создать задачу в рабочей области папки **Задачи**:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите мастер создания задачи по кнопке **Готово**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

### См. также

Сценарий: Мониторинг и отчеты ..... 576
Сценарий: Настройка защиты сети ..... 400

## Создание задачи Сервера администрирования

Сервер администрирования выполняет следующие функции:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных;
- синхронизация обновлений Windows Update;
- создание инсталляционного пакета на основе образа операционной системы эталонного устройства.

На виртуальном Сервере администрирования доступна только задача автоматической рассылки отчетов и задача создания инсталляционного пакета на основе образа операционной системы эталонного устройства. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования. Резервное копирование данных виртуального Сервера осуществляется в рамках резервного копирования данных главного Сервера администрирования.

► *Чтобы создать задачу Сервера администрирования:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Новый** → **Задачу**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Задачи Загрузка обновлений в хранилище Сервера администрирования, Синхронизация обновлений Windows Update, Обслуживание базы данных и *Резервное копирование данных Сервера администрирования* можно создать только в одном экземпляре. Если задачи *Загрузка обновлений в хранилище Сервера администрирования*, *Обслуживание базы данных*, *Резервное копирование данных Сервера администрирования* и *Синхронизация обновлений Windows Update* уже созданы для Сервера администрирования, то они не отображаются в окне выбора типа задачи мастера создания задачи.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Создание задачи для набора устройств

В Kaspersky Security Center можно создавать задачи для произвольно выбранного набора устройств. Устройства в наборе могут входить в разные группы администрирования или не входить ни в одну группу администрирования. Kaspersky Security Center позволяет выполнять следующие основные задачи для набора устройств:

- Удаленная установка программ (см. стр. 362).
- Отправка сообщения для пользователя (см. стр. 727).
- Смена Сервера администрирования (см. стр. 724).
- Управление устройствами (см. стр. 725).
- Проверка обновлений (см. стр. 470).
- Распространение инсталляционных пакетов (см. стр. 378).
- Удаленная установка программы на подчиненные Серверы администрирования (см. стр. 365).
- Удаленная деинсталляция программ (см. стр. 370).

► *Чтобы создать задачу для набора устройств:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Новый → Задача**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Создание локальной задачи

► *Чтобы создать локальную задачу для устройства:*

1. В рабочей области группы, в состав которой входит устройство, выберите закладку **Устройства**.
2. В списке устройств на закладке **Устройства** выберите устройство, для которого нужно создать локальную задачу.
3. Запустите процесс создания задачи для выбранного устройства одним из следующих способов:
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Создать задачу**.
   - В рабочей области папки Задачи нажмите на кнопку **Создать задачу**.
   - Используйте свойства устройства следующим образом:
     a. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
     b. В открывшемся окне свойств устройства выберите раздел **Задачи** и нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Подробные описания создания и настройки локальных задач приводятся в Руководствах к соответствующим программам "Лаборатории Касперского".

### См. также:

Сценарий: Настройка защиты сети .....400

## Отображение унаследованной групповой задачи в рабочей области вложенной группы

► *Чтобы включить отображение унаследованных задач вложенной группы в рабочей области:*

1. Выберите в рабочей области вложенной группы закладку **Задачи**.
2. В рабочей области закладки **Задачи** нажмите на кнопку **Показывать унаследованные задачи**.

В результате унаследованные задачи отображаются в списке задач со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования редактирование унаследованных задач доступно только в той группе, в которой они были созданы. Редактирование унаследованных задач недоступно в той группе, которая наследует задачи.

### См. также:

Сценарий: Настройка защиты сети .....400

## Автоматическое включение устройств перед запуском задачи

Kaspersky Security Center не выполняет задачи на выключенных устройствах. Вы можете настроить Kaspersky Security Center на автоматическое включение этих устройств перед запуском задачи с помощью функции Wake-on-LAN.

► *Чтобы настроить автоматическое включение устройств перед запуском задачи:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Чтобы настроить действия на устройствах, перейдите по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Активировать устройство перед запуском задачи функцией Wake-On-Lan за (мин)** и укажите время в минутах.

В результате за указанное количество минут до запуска задачи, Kaspersky Security Center включает устройства и загружает операционную систему с помощью функции Wake-on-LAN. После выполнения задачи устройства автоматически выключаются, если пользователи устройств не входят в систему. Kaspersky Security Center автоматически выключает только те устройства, которые включены с помощью функции Wake-on-LAN.

Kaspersky Security Center может автоматически запускать операционные системы только на устройствах, поддерживающих стандарт Wake-on-LAN (WoL).

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Автоматическое выключение устройства после выполнения задачи

Kaspersky Security Center позволяет настроить параметры задачи таким образом, чтобы после ее выполнения устройства, на которые она распространяется, автоматически выключались.

► *Чтобы устройства автоматически выключались после выполнения задачи:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Выключать устройство после выполнения задачи**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

### Ограничение времени выполнения задачи

► *Чтобы ограничить время выполнения задачи на устройствах:*

1. В окне свойств задачи выберите раздел **Расписание**.
2. Откройте окно настройки действий с клиентскими устройствами по ссылке **Дополнительно**.
3. В открывшемся окне **Дополнительно** установите флажок **Остановить, если задача выполняется дольше (мин)** и укажите время в минутах.

В результате, если по истечении указанного времени выполнение задачи на устройстве не будет завершено, Kaspersky Security Center автоматически остановит выполнение задачи.

См. также:

Сценарий: Настройка защиты сети ..... 400

### Экспорт задачи

Вы можете экспортировать групповые задачи и задачи для наборов устройств в файл. Задачи Сервера администрирования и локальные задачи недоступны для экспорта.

► *Чтобы экспортировать задачу:*

1. В контекстном меню задачи выберите пункт **Все задачи** → **Экспортировать**.
2. В открывшемся окне **Сохранить как** укажите имя файла и путь для сохранения.
3. Нажмите на кнопку **Сохранить**.

Права локальных пользователей не экспортируются.

См. также:

Сценарий: Настройка защиты сети ..... 400

### Импорт задачи

Вы можете импортировать групповые задачи и задачи для наборов устройств. Задачи Сервера администрирования и локальные задачи недоступны для импорта.

► *Чтобы импортировать задачу:*

1. Выберите список задач, в который требуется импортировать задачу:
   - Если вы хотите импортировать задачу в список групповых задач, в рабочей области нужной вам группы администрирования выберите закладку **Задачи**.
   - Если вы хотите импортировать задачу в список задач для наборов устройств, в дереве консоли выберите папку **Задачи**.
2. Выберите один из следующих способов импорта задачи:

- В контекстном меню списка задач выберите пункт **Все задачи** → **Импортировать**.
- По ссылке **Импортировать задачу из файла** в блоке управления списком задач.

3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать задачу.
4. Нажмите на кнопку **Открыть**.

В результате импортированная задача отобразится в списке задач.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Конвертация задач

С помощью Kaspersky Security Center можно конвертировать задачи предыдущих версий программ "Лаборатории Касперского" в задачи текущих версий программ.

Конвертация возможна для задач следующих программ:

- Антивирус Касперского 6.0 для Windows Workstations MP4;
- Kaspersky Endpoint Security 8 для Windows;
- Kaspersky Endpoint Security 10 для Windows.

► *Чтобы конвертировать задачи:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию задач.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

   В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

В результате работы мастера формируются новые задачи, использующие параметры задач предыдущих версий программ.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Запуск и остановка задачи вручную

Задачи можно запускать и останавливать двумя способами: из контекстного меню задачи и в окне свойств клиентского устройства, которому назначена эта задача.

Запускать групповые задачи из контекстного меню устройства могут пользователи, входящие в группу **KLAdmins** (см. стр. 675).

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств задачи:*

1. В списке задач выберите задачу.
2. Запустите или остановите задачу одним из следующих способов:
   - В контекстном меню задачи выберите пункт **Запустить** или **Остановить**.
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Запустить** или **Остановить**.

► *Чтобы запустить или остановить задачу из контекстного меню или окна свойств клиентского устройства:*

1. В списке устройств выберите устройство.
2. Запустите или остановите задачу одним из следующих способов:
   - В контекстном меню устройства выберите пункт **Все задачи** → **Запустить задачу**. Из списка задач выберите требуемую.

     Список устройств, для которых назначена задача, будет замещен выбранным устройством. Задача будет запущена.
   - В окне свойств устройства в разделе **Задачи** нажмите на кнопку запуска (  ) или остановки (  ).

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Приостановка и возобновление задачи вручную

► *Чтобы приостановить или возобновить выполнение запущенной задачи:*

1. В списке задач выберите задачу.
2. Приостановите или возобновите выполнение задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Приостановить** или **Возобновить**.
   - В разделе **Общие** окна свойств задачи нажмите на кнопку **Приостановить** или **Возобновить**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Наблюдение за ходом выполнения задачи

► *Чтобы наблюдать за ходом выполнения задачи,*

В окне свойств задачи выберите раздел **Общие**.

В средней части окна раздела **Общие** содержится информация о текущем состоянии задачи.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Просмотр результатов выполнения локальных задач недоступен.

► *Чтобы посмотреть результаты выполнения задачи:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка фильтра информации о результатах выполнения задачи

Kaspersky Security Center позволяет фильтровать информацию о результатах выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Для локальных задач фильтрация недоступна.

► *Чтобы настроить фильтр для информации о результатах выполнения задачи:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

   Таблица в верхней части окна содержит список всех устройств, для которых назначена задача. Таблица в нижней части окна содержит результаты выполнения задачи на выбранном устройстве.
3. В интересующей вас таблице по правой клавише мыши откройте контекстное меню и выберите в нем пункт **Фильтр**.
4. В открывшемся окне **Применить фильтр** настройте параметры фильтра в разделах окна **События**, **Устройства** и **Время**. Нажмите на кнопку **ОК**.

В результате в окне **Результаты выполнения задачи** будет отображаться информация, удовлетворяющая параметрам, заданным в фильтре.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Изменение задачи. Откат изменений

► *Чтобы изменить задачу:*

1. В дереве консоли выберите папку **Задачи**.

2. В рабочей области папки **Задачи** выберите задачу и с помощью контекстного меню перейдите в окно свойств задачи.
3. Внесите необходимые изменения.

   В разделе **Исключения из области действия задачи** можно настроить список вложенных групп, на которые не будет распространяться задача.

4. Нажмите на кнопку **Применить**.

Изменения задачи будут сохранены в окне свойств задачи, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения задачи.

► *Чтобы откатить изменения задачи:*

1. В дереве консоли выберите папку **Задачи**.
2. Выберите задачу, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств задачи.
3. В окне свойств задачи выберите раздел **История ревизий**.
4. В списке ревизий задачи выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Сравнение задач

Вы можете сравнивать задачи одного типа, например, можно сравнить две задачи поиска вредоносного ПО, но нельзя сравнить задачу поиска вредоносного ПО с задачей установки обновлений. В результате сравнения задач вы получаете отчет, показывающий, какие параметры задач совпадают, а какие различаются. Вы можете распечатать отчет сравнения задач или сохранить его в файле. Сравнение задач может потребоваться в случае, когда для разных подразделений одной компании есть различные задачи одного типа. Например, для бухгалтерии есть задача поиска вредоносного ПО только на локальных дисках компьютера, а для отдела продаж, сотрудники которого переписываются с клиентами, есть задача проверять и локальные диски, и почту. Чтобы быстро увидеть такие различия, нет необходимости просматривать все параметры задачи, достаточно выполнить сравнение задач.

Сравнение можно выполнить только для задач одного типа.
Задачи можно сравнивать только попарно.

Вы можете сравнивать задачи одним из следующих способов: путем выбора одной задачи и сравнения ее с другой или путем сравнения любых двух задач из списка задач.

► *Чтобы выбрать одну задачу и сравнить ее с другой:*

1. В дереве консоли выберите папку **Задачи**.

2. В рабочей области папки **Задачи** выберите задачу, которую нужно сравнить с другой задачей.
3. В контекстном меню задачи выберите пункт **Все задачи** → **Сравнить с другой задачей**.
4. В окне **Выбор задачи** выберите задачу для сравнения.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух задач в формате HTML.

► *Чтобы сравнить две задачи из списка задач:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** в списке задач с помощью клавиши **SHIFT** или **CTRL** выберите две задачи одного типа.
3. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения выбранных задач в формате HTML.

При сравнении задач, в случае если используемые пароли отличаются, в отчете сравнения задач будут отображаться символы ******.

Если в свойствах задачи был изменен пароль, в отчете сравнения ревизий задачи будут отображаться символы ******.

### См. также:

Сценарий: Настройка защиты сети .....400

## Учетные записи для запуска задач

Вы можете задавать учетную запись, под которой должна запускаться задача.

Например, для выполнения задач проверки по требованию необходимы права на доступ к проверяемому объекту, а для выполнения задач обновления – права авторизованного пользователя прокси-сервера. Возможность задать учетную запись для запуска задачи позволяет избежать ошибки при выполнении задач проверки по требованию и задач обновления, если у пользователя, запустившего задачу, нет необходимых прав доступа.

В задачах удаленной установки и деинсталляции программы учетная запись используется для загрузки на клиентские устройства файлов, необходимых для установки (удаления), если на устройстве не установлен или недоступен Агент администрирования. При установленном и доступном Агенте администрирования учетная запись используется, если согласно параметрам задачи доставка файлов выполняется только средствами Microsoft Windows из папки общего доступа. В этом случае учетная запись должна обладать следующими правами на устройстве:

- правом на удаленный запуск программ;
- правами на ресурс Admin$;
- правом *Вход в качестве службы*.

Если доставку файлов на устройства выполняет Агент администрирования, учетная запись использоваться не будет. Все операции по копированию и установке файлов будет выполнять **Агент администрирования** (**Учетная запись LocalSystem**).

## См. также:



## Мастер изменения паролей задач

Для не-локальной задачи можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете сделать это вручную в свойствах каждой задачи.

► *Чтобы запустить мастер изменения паролей задач:*

1. В дереве консоли выберите узел **Задачи**.
2. В контекстном меню узла выберите пункт **Мастер изменения паролей задач**.

Следуйте далее указаниям мастера.

## В этом разделе



## Шаг 1. Выбор учетных данных

В полях **Учетная запись** и **Пароль** укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

При заполнении поля **Старый пароль (необязательно)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

## См. также:

### Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали старый пароль или указанный старый пароль не соответствует паролям задач, необходимо выбрать действие, выполняемое с этими задачами.

Для каждой задачи со статусом *Требуется одобрение* определите, хотите ли вы удалить пароль в свойствах задачи или заменить его на новый. Если вы выберите удаление пароля, задача перейдет в режим запуска с правами учетной записи, заданной по умолчанию.

### См. также:



### Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

### См. также:



## Создание иерархии групп администрирования, подчиненных виртуальному Серверу администрирования

После создания виртуального Сервера администрирования он по умолчанию содержит группу администрирования **Управляемые устройства**.

Процедура создания иерархии групп администрирования, подчиненных виртуальному Серверу администрирования, совпадает с процедурой создания иерархии групп администрирования, подчиненных физическому Серверу администрирования (см. стр. 81).

В состав групп администрирования, подчиненных виртуальному Серверу администрирования, нельзя добавлять подчиненные и виртуальные Серверы администрирования. Это связано с ограничениями виртуальных Серверов администрирования (см. стр. 169).

### См. также:

kaspersky

# Политики и профили политик

В Kaspersky Security Center 14.2 Web Console можно создавать политики для программ "Лаборатории Касперского" (см. стр. 69). В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

## В этом разделе



## См. также:



## Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В разделе также содержится информация о профилях политик.

## В этом разделе



## Иерархия политик

В Kaspersky Security Center политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики программы P, определенной для группы G, являются управляемые устройства с установленной программой P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" ( ) возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одной и той же программы действуют друг на друга по иерархии групп администрирования: параметры с установленным "замком" из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Политика для автономных пользователей не будет поддерживаться в будущих версиях Kaspersky Security Center. Вместо политик для автономных пользователей следует использовать профили политик.

## Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Во избежание подобных проблем в Kaspersky Security Center поддерживаются *профили политики*. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров политики распространяется на устройства вместе с политикой и дополняет политику при выполнении некоторого условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

### Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования (см. стр. 306);
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);

  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля содержат разные значения одного и того же параметра, возникает неоднозначность. Неоднозначность устраняется при помощи приоритетов профилей: значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

**Поведение профилей при действии политик друг на друга по иерархии**

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

## Наследование параметров политики

Политика задается для группы администрирования. Параметры политики могут *наследоваться*, то есть передаваться в подгруппы (дочерние группы) групп администрирования, для которых она создана. Политика, созданная для родительской группы, также называется *родительской политикой*.

Можно включить или выключить два параметра наследования: **Наследовать параметры родительской политики** и **Обеспечить принудительное наследование параметров для дочерних политик**.

- Если вы включили **Наследовать параметры родительской политики** для дочерней политики и заблокировали некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры для дочерней группы. Однако вы можете изменить параметры, которые не заблокированы в родительской политике.
- Если вы выключили **Наследовать параметры родительской политики** для дочерней политики, тогда вы можете изменить все параметры в дочерней группе, даже если некоторые параметры заблокированы в родительской политике.
- Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.
- В политиках для группы **Управляемые устройства** параметр **Наследовать параметры родительской политики** не влияет ни на какие параметры, так как группа **Управляемые устройства** не имеет вышестоящих групп и, следовательно, не наследует никакие политики.

По умолчанию параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

## Управление политиками

Централизованная настройка параметров программ, установленных на клиентских устройствах, осуществляется через определение политик.

Политики, сформированные для программ в группе администрирования, отображаются в рабочей области на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (см. стр. 903).

После удаления политики или прекращения ее действия программа продолжает работу с параметрами, заданными в политике. В дальнейшем эти параметры можно изменить вручную.

Применение политики производится следующим образом: если на устройстве выполняются резидентные задачи (задачи постоянной защиты), их выполнение продолжается с новыми значениями параметров. Запущенные периодические задачи (проверка по требованию, обновление баз программ) выполняются с неизмененными значениями. Новый запуск периодических задач производится с измененными значениями параметров.

Политики для программ с поддержкой мультитенантности наследуются для групп администрирования более низкого уровня, а также для групп администрирования верхнего уровня: политика распространяется на все клиентские устройства, на которых установлена программа.

В случае использования иерархической структуры Серверов администрирования подчиненные Серверы получают политики с главного Сервера администрирования и распространяют их на клиентские устройства. При включенном механизме наследования параметры политики можно изменять на главном Сервере администрирования. После этого изменения, внесенные в параметры политики, распространяются на унаследованные политики на подчиненных Серверах администрирования.

При разрыве соединения между главным и подчиненным Серверами администрирования политика на подчиненном Сервере продолжает действовать с прежними параметрами. Параметры политики, измененные на главном Сервере администрирования, распространятся на подчиненный Сервер после восстановления соединения.

При отключенном механизме наследования параметры политики можно изменять на подчиненном Сервере независимо от главного Сервера.

Если происходит разрыв соединения между Сервером администрирования и клиентским устройством, на устройстве вступает в силу политика для автономного пользователя (если она определена), или политика продолжает действовать с прежними параметрами до восстановления соединения.

Результаты распространения политики на подчиненные Серверы администрирования отображаются в окне свойств политики на главном Сервере администрирования.

Результаты распространения политики на клиентские устройства отображаются в окне свойств политики Сервера администрирования, к которому они подключены.

Не используйте в параметрах политик конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

kaspersky

## В этом разделе



## Создание политики

В Консоли администрирования можно создавать политики непосредственно в папке группы администрирования, для которой создается политика, и в рабочей области папки **Политики**.

► *Чтобы создать политику в папке группы администрирования:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите закладку **Политики**.
3. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

► *Чтобы создать политику в рабочей области папки **Политики**:*

1. В дереве консоли выберите папку **Политики**.
2. Запустите мастер создания политики по кнопке **Новая политика**.

В результате запускается мастер создания политики. Следуйте далее указаниям мастера.

Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика становится неактивной.

При создании политики можно настроить минимальный набор параметров, без которых программа не будет работать. Остальные значения параметров устанавливаются по умолчанию и соответствуют значениям по умолчанию при локальной установке программы. Вы можете изменять политику после ее создания.

Не используйте в параметрах политик конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

Параметры программ "Лаборатории Касперского", которые изменяются после применения политик, подробно описаны в Руководствах к каждой из них.

После создания политики параметры, на изменение которых наложен запрет (установлен "замок" ), начинают действовать на клиентских устройствах независимо от того, какие параметры были определены для программы ранее.

### См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

## Отображение унаследованной политики во вложенной группе

► *Чтобы включить отображение унаследованных политик для вложенной группы администрирования:*

1. В дереве консоли выберите группу администрирования, для которой нужно отображать унаследованные политики.
2. В рабочей области группы выберите закладку **Политики**.
3. В контекстном меню списка политик выберите пункт **Вид → Унаследованные политики**.

В результате унаследованные политики отображаются в списке политик со значком:

-  – если они были унаследованы от группы, созданной на главном Сервере администрирования;
-  – если они были унаследованы от группы верхнего уровня.

При включенном режиме наследования параметров изменение унаследованных политик доступно только в той группе, в которой они были созданы. Изменение унаследованных политик недоступно в той группе, которая наследует политики.

## Активация политики

► *Чтобы сделать политику активной для выбранной группы:*

1. В рабочей области группы на закладке **Политики** выберите политику, которую нужно сделать активной.
2. Для активации политики выполните одно из следующих действий:
   - В контекстном меню политики выберите пункт **Активная политика**.

- В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Активная политика**.

В результате политика становится активной для выбранной группы администрирования.

При применении политики на большом количестве клиентских устройств на некоторое время существенно возрастают нагрузка на Сервер администрирования и объем сетевого трафика.

## Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":*

1. В окне свойств Сервера администрирования откройте раздел **Вирусная атака**.
2. Откройте окно **Активация политик** по ссылке **Настроить активацию политик по возникновению события "Вирусная атака"** и добавьте политику в выбранный список политик, активируемых при обнаружении вирусной атаки.

В случае активации политики по событию *Вирусная атака* вернуться к предыдущей политике можно только вручную.

## Применение политики для автономных пользователей

Политика для автономных пользователей вступает в силу на устройстве в случае его отключения от сети организации.

► *Чтобы применить политику для автономных пользователей:*

В окне свойств политики откройте раздел **Общие** и в блоке параметров **Состояние политики** выберите вариант **Политика для автономных пользователей**.

В результате политика для автономных пользователей начинает действовать на устройствах в случае их отключения от сети организации.

## Изменение политики. Откат изменений

► *Чтобы изменить политику:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
3. Внесите необходимые изменения.
4. Нажмите на кнопку **Применить**.

Изменения политики будут сохранены в свойствах политики, в разделе **История ревизий**.

В случае необходимости вы можете откатить изменения политики.

► *Чтобы откатить изменения политики:*

1. В дереве консоли выберите папку **Политики**.
2. Выберите политику, изменения которой нужно откатить и с помощью контекстного меню перейдите в окно свойств политики.
3. В окне свойств политики выберите раздел **История ревизий**.
4. В списке ревизий политики выберите номер ревизии, к которой нужно откатить изменения.
5. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

## Сравнение политик

Вы можете сравнивать две политики для одной управляемой программы. В результате сравнения политик вы получаете отчет, показывающий, какие параметры политик совпадают, а какие различаются. Сравнивать политики бывает нужно, например, если разные администраторы в своих локальных офисах создали несколько политик для одной управляемой программы или если одна политика верхнего уровня была унаследована и изменена для каждого локального офиса. Вы можете сравнивать политики одним из следующих способов: путем выбора одной политики и сравнения ее с другой или путем сравнения любых двух политик из списка политик.

► *Чтобы сравнить политику с другой политикой:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику, которую нужно сравнить с другой политикой.
3. В контекстном меню политики выберите пункт **Сравнить политику с другой политикой**.
4. В окне **Выбор политики** выберите политику, с которой нужно провести сравнение.
5. Нажмите на кнопку **ОК**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

► *Чтобы сравнить две политики из списка политик:*

1. В папке **Политики** в списке политик с помощью клавиши **SHIFT** или **CTRL** выберите две политики для одной управляемой программы.
2. В контекстном меню выберите пункт **Сравнить**.

Отобразится отчет сравнения двух политик для программы в формате HTML.

В отчете сравнения параметров политик для программы Kaspersky Endpoint Security для Windows выполняется также сравнение профилей политики. Результаты сравнения параметров профилей политик можно свернуть. Чтобы свернуть блок, нажмите на значок стрелки (▲) рядом с названием блока.

## Удаление политики

► *Чтобы удалить политику:*

1. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую нужно удалить.
2. Удалите политику одним из следующих способов:

- В контекстном меню политики выберите пункт **Удалить**.
- Перейдите по ссылке **Удалить политику** в информационном окне выбранной политики.

## Копирование политики

► *Чтобы скопировать политику:*

1. В рабочей области нужной вам группы на закладке **Политики** выберите политику.
2. В контекстном меню политики выберите пункт **Копировать**.
3. Выберите в дереве консоли группу, в которую требуется добавить политику.

   Политику можно добавить в ту же группу, из которой она скопирована.
4. В контекстном меню списка политик для выбранной группы на закладке **Политики** выберите пункт **Вставить**.

В результате политика копируется с сохранением всех параметров и распространяется на устройства группы, в которую она перенесена. Если вы вставляете политику в ту же группу, из которой она была скопирована, индекс **(<следующий порядковый номер>)** автоматически добавляется к имени политики, например: **(1)**, **(2)**.

Активная политика при копировании становится неактивной. В случае необходимости вы можете сделать ее активной.

## Экспорт политики

► *Чтобы экспортировать политику:*

1. Экспортируйте политику одним из следующих способов:
   - В контекстном меню списка политик выберите пункт **Все задачи → Импортировать**.
   - Перейдите по ссылке **Экспорт политики в файл** в информационном окне для выбранной политики.
2. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

## Импорт политики

► *Чтобы импортировать политику:*

1. В рабочей области нужной вам группы на закладке **Политики** выберите один из следующих способов импорта политики:
   - В контекстном меню списка политик выберите пункт **Все задачи → Импорт**.
   - По кнопке **Импортировать политику из файла** в блоке управления списком политик.
2. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать политику. Нажмите на кнопку **Открыть**.

Импортированная политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

## Конвертация политик

Kaspersky Security Center может конвертировать политики предыдущих версий программ "Лаборатории Касперского" в политики текущих версий этих программ. Преобразованные политики сохраняют текущие параметры администратора, заданные до обновления, а также включают новые параметры из актуальных версий программ. Плагины управления программами "Лаборатории Касперского" определяют, доступна ли конвертация политик этих программ. Информацию о конвертации политик для каждой поддерживаемой программы "Лаборатории Касперского" см. в соответствующей справке из следующего списка:

- **Программы "Лаборатории Касперского" для рабочих станций:**
  - Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/134238.htm
  - Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/233554.htm
  - Kaspersky Endpoint Security для Linux Elbrus Edition https://support.kaspersky.com/help/KES4LinuxElbrus/10.1.2/ru-RU/180528.htm
  - Kaspersky Endpoint Security для Linux ARM Edition https://support.kaspersky.com/help/KES4LinuxARM/10.1.4/ru-RU/208976.htm
  - Kaspersky Endpoint Security для Mac https://support.kaspersky.com/KESMac/11.2.1_adminguide/ru-RU/180604.htm
  - Kaspersky Endpoint Agent https://support.kaspersky.com/KEA/3.13/ru-RU/232801.htm
  - Kaspersky Embedded Systems Security для Windows https://support.kaspersky.com/KESS/3.0/ru-RU/146617.htm
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes https://support.kaspersky.com/KICS4Nodes/3.1/ru-RU/146617.htm
  - Kaspersky Industrial CyberSecurity for Linux Nodes https://support.kaspersky.com/help/KICS4Linux/1.3/ru-RU/233542.htm
  - Kaspersky Industrial CyberSecurity for Networks (централизованное развертывание не поддерживается) https://support.kaspersky.com/help/KICSforNetworks/3.1/ru-RU/140030.htm
- **Программы "Лаборатории Касперского" для мобильных устройств:**
  - Kaspersky Endpoint Security для Android https://support.kaspersky.com/KESMob/10SP4MR3/ru-RU/99183.htm
  - Kaspersky Security для iOS https://support.kaspersky.com/KESMob/10SP4MR3/ru-RU/99183.htm
- **Программы "Лаборатории Касперского" для файловых серверов:**

  - Kaspersky Security для Windows Server https://support.kaspersky.com/KSWS/11.0.1/ru-RU/146617.htm
  - Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/134238.htm
  - Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/233554.htm
- **Программы "Лаборатории Касперского" для виртуальных машин:**
  - Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/5.2/ru-RU/62771.htm
  - Kaspersky Security для виртуальных сред Защита без агента https://support.kaspersky.ru/KSV/5.0/ru-RU/84556.htm
- **Программы "Лаборатории Касперского" для почтовых систем и серверов SharePoint/серверов совместной работы:**
  - Kaspersky Security для Linux Mail Server https://support.kaspersky.com/KLMS/8.2/ru-RU/100512.htm
  - Kaspersky Security для Microsoft Exchange Servers https://support.kaspersky.com/KS4Exchange/9.6/ru-RU/131648.htm
- **Программы "Лаборатории Касперского" для обнаружения целевых атак:**
  - Kaspersky Sandbox https://support.kaspersky.com/KSB/2.0/ru-RU/189564.htm
  - Kaspersky Endpoint Detection and Response Optimum https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/220194.htm
  - Kaspersky Managed Detection and Response https://support.kaspersky.com/MDR/ru-RU/196544.htm
- **Программы "Лаборатории Касперского" для устройств с KasperskyOS:**
  - Kaspersky IoT Secure Gateway https://support.kaspersky.com/IoTSecureGateway/2.1/ru-RU/188039.htm
  - Kaspersky Security Management Suite (плагин для Kaspersky Thin Client) https://support.kaspersky.com/help/KTC/1.5/ru-RU/231960.htm

► *Чтобы конвертировать политики:*

1. В дереве консоли выберите Сервер администрирования, для которого вы хотите выполнить конвертацию политик.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер массовой конвертации политик и задач**.

В результате запускается мастер массовой конвертации политик и задач. Следуйте далее указаниям мастера.

После завершения работы мастера создаются политики, использующие текущие параметры политик администратора и новые параметры из актуальных версий программ "Лаборатории Касперского".

## Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, изменении

профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

## В этом разделе



## О профиле политики

Профиль политики – это именованный набор параметров политики, который активируется на клиентском устройстве (компьютере, мобильном устройстве), если устройство удовлетворяет заданным правилам активации (см. стр. 441). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политики нужны для того, чтобы устройства внутри одной группы администрирования могли иметь разные параметры политики. Например, возможна ситуация, когда в группе администрирования для некоторых устройств параметры политики должны быть изменены. В этом случае для такой политики можно настроить профили политики, использование которых позволяет изменять параметры политики не для всех устройств группы администрирования. Например, политика запрещает запуск программ городской навигации для всех устройств группы администрирования "Пользователи". Программы городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". На этом устройстве можно установить тег "Курьер" и настроить профиль политики таким образом, чтобы был разрешен запуск программ городской навигации только на устройстве с тегом "Курьер", с сохранением всех остальных параметров политики. В этом случае если в группе администрирования "Пользователи" появляется устройство с тегом "Курьер", на нем будет разрешен запуск программ городской навигации. Запуск программ городской навигации на других устройствах в группе администрирования "Пользователи", у которых тег "Курьер" отсутствует, будет запрещен.

Профили поддерживаются только для следующих политик:

- политики Kaspersky Endpoint Security для Windows;
- политики Kaspersky Endpoint Security для Mac;
- политики плагина Kaspersky Mobile Device Management версий от 10 Service Pack 1 до 10 Service Pack 3 Maintenance Release 1;
- политики плагина Kaspersky Device Management для iOS;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows;
- политики Kaspersky Security для виртуальных сред 5.1 Легкий агент для Linux.

Профили политик облегчают управление клиентскими устройствами, на которых применены политики:

- Параметры профиля политики могут отличаться от параметров самой политики.
- Не требуется поддерживать и применять вручную несколько копий одной политики, которые различаются только небольшим количеством параметров.
- Не требуется отдельная политика для автономных пользователей.

- Вы можете экспортировать и импортировать профили политики, а также создавать новые профили на основе существующих.
- Для одной политики несколько профилей политики могут быть активными. К устройству будут применены те из профилей, которые удовлетворяют правилам активации на этом устройстве.
- Профили подчиняются иерархии политик. Унаследованная политика содержит все профили политики верхнего уровня.

**Приоритеты профилей**

Профили, созданные для политики, упорядочены в порядке убывания приоритета. Например, если профиль X находится выше профиля Y в списке профилей, то профиль X имеет более высокий приоритет, чем Y. К одному устройству одновременно могут быть применены несколько профилей. Если значение какого-то параметра различается в профилях, на устройстве применится значение параметра из того профиля, который имеет более высокий приоритет.

**Правила активации профиля**

Профиль политики активируется на клиентском устройстве при выполнении правила активации. *Правила активации* – набор условий, при выполнении которых профиль политики начинает работать на устройстве. Правило активации может содержать следующие условия:

- Агент администрирования на клиентском устройстве подключается к Серверу с определенным набором параметров подключения, например, адрес Сервера, номер порта и так далее.
- Клиентское устройство находится в автономном режиме.
- Клиентскому устройству назначены определенные теги.
- Клиентское устройство явно (устройство находится непосредственно в указанном подразделении) или неявно (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности) размещено в определенном подразделении Active Directory®, устройство или его владелец находятся в группе безопасности Active Directory.
- Клиентское устройство принадлежит определенному владельцу или владелец устройства находится во внутренней группе безопасности Kaspersky Security Center.
- Владельцу устройства была назначена определенная роль.

**Политики в иерархии групп администрирования**

Если вы создаете политику в группе администрирования нижнего уровня, то новая политика наследует профили активной политики для группы верхнего уровня. Профили с одинаковыми именами объединяются. Профили политики для группы более высокого уровня имеют более высокий приоритет. Например, в группе администрирования *A* политика *P(A)* имеет профили *X1*, *X2*, и *X3*, в порядке убывания приоритета. В группе администрирования *B*, которая является подгруппой группы *A*, создана политика *P(B)*, с профилями *X2*, *X4*, *X5*. Тогда политика *P(B)* будет изменена политикой *P(A)* так, что в политике *P(B)* список профилей будет выглядеть следующим образом: *X1*, *X2*, *X3*, *X4*, *X5* (в порядке убывания приоритета). Приоритет профиля *X2* будет зависеть от начального состояния *X2* политики *P(B)* и *X2* политики *P(A)*. После создания политики *P(B)* политика *P(A)* не будет отображаться в подгруппе *B*.

Активная политика вычисляется каждый раз заново при запуске Агента администрирования, при включении и выключении автономного режима, а также при изменении списка тегов, назначенных клиентскому устройству. Например, устройству увеличили объем оперативной памяти, в результате активировался профиль политики, который применяется для устройств с большим объемом оперативной памяти.

**Свойства и ограничения профиля политики**

Профили имеют следующие свойства:

- Профили неактивной политики не влияют на клиентские устройства.
- Если для политики установлено состояние **Для автономных пользователей**, профили политики также будут применяться при отключении устройства от корпоративной сети.
- Профили не поддерживают статический анализ доступа к исполняемым файлам (см. стр. 568).
- Профиль политики не может содержать параметры оповещений о событиях.
- Если используется UDP-порт 15000 для подключения устройства к Серверу администрирования, то при назначении тега устройству соответствующий профиль политики активируется в течение одной минуты.
- Вы можете использовать правила подключения Агента администрирования к Серверу администрирования (см. стр. 311), когда вы создаете правила активации профиля политики.

## Создание профиля политики

Создание профиля доступно только для политик следующих программ:

- Kaspersky Endpoint Security 10 Service Pack 1 для Windows и выше;
- Kaspersky Endpoint Security 10 Service Pack 1 для Mac;
- плагина Kaspersky Mobile Device Management до версий 10 Service Pack 3 Maintenance Release 1;
- плагина Kaspersky Device Management для iOS;
- Kaspersky Security для виртуальных сред 5.1 Легкий агент для Windows и Linux.

► *Чтобы создать профиль политики:*

1. В дереве консоли выберите группу администрирования, для политики которой нужно создать профиль политики.
2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики и нажмите на кнопку **Добавить**.

   Запустится мастер создания профиля политики.
5. В окне мастера **Имя профиля политики** укажите:
   a. Имя профиля политики.

      Имя профиля не может превышать 100 символов.

   b. Состояние профиля политики (*Включен* или *Выключен*).

      Рекомендуется создавать неактивные профили политики и включать их только после полного завершения настройки параметров и условий активации профилей политики.
6. Установите флажок **После закрытия мастера создания профиля политики перейти к настройке правила активации профиля политики**, чтобы запустить мастер создания правила активации профиля политики (см. стр. 441). Следуйте инструкциям мастера.
7. Измените параметры профиля политики в окне свойств профиля политики (см. стр. 440), как вам необходимо.

8. Сохраните изменения, нажав на кнопку **ОК**.

   Профиль будет сохранен. Профиль будет активирован на устройствах, удовлетворяющих правилам активации.

Для одной политики можно создать несколько профилей политики. Профили, созданные для политики, отображаются в свойствах политики в разделе **Профили политики**. Вы можете изменить профиль политики и приоритет профиля (см. стр. 440), а также удалить профиль (см. стр. 441).

## См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

## Изменение профиля политики

### Изменение параметров профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

► *Чтобы изменить профиль политики:*

1. В дереве консоли выберите группу администрирования, для которой нужно изменить профиль политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики.

   В разделе содержится список профилей, созданных для политики. Профили в списке отображаются в соответствии с их приоритетом.
5. Выберите профиль политики и нажмите на кнопку **Свойства**.
6. В окне свойств настройте параметры профиля:
   - Если необходимо, в разделе **Общие** измените имя профиля и включите или выключите профиль с помощью флажка **Включить профиль**.
   - В разделе **Правила активации** измените правила активации профиля.
   - Измените параметры политики в соответствующих разделах.
7. Нажмите на кнопку **ОК**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

### Изменение приоритета профиля политики

Приоритет профилей политик определяет порядок активации профилей на клиентском устройстве. Приоритет используется, если для разных профилей политики заданы одинаковые правила активации.

Например, созданы два профиля политики: *Профиль 1* и *Профиль 2*, отличающиеся друг от друга значениями одного параметра (*Значение 1* и *Значение 2*). Приоритет *Профиля 1* выше, чем приоритет *Профиля 2*. Кроме

того, существуют профили с более низким приоритетом, чем *Профиль 2*. Правила активации профилей совпадают.

При выполнении правила активации будет активирован *Профиль 1*. Параметр на устройстве примет *Значение 1*. Если удалить *Профиль 1,* то *Профиль 2,* будет иметь самый высокий приоритет, и параметр примет *Значение 2*.

В списке профилей политики профили отображаются в соответствии с их приоритетом. На первом месте в списке стоит профиль с самым высоким приоритетом. Приоритет профиля можно изменять с помощью кнопок со стрелкой вверх  и со стрелкой вниз  .

## Удаление профиля политики

► *Чтобы удалить профиль политики:*

1. Выберите в дереве консоли группу администрирования, для которой нужно удалить профиль политики.
2. В рабочей области группы администрирования выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Откройте раздел **Профиль политики** в свойствах политики Kaspersky Endpoint Security.
5. Выберите профиль политики, который нужно удалить, и нажмите на кнопку **Удалить**.

В результате профиль политики будет удален. Активным станет либо другой профиль политики, правила активации которого выполняются на устройстве, либо политика.

## Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики:*

1. В дереве консоли выберите группу администрирования, для которой нужно создать правило активации профиля политики.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику и с помощью контекстного меню перейдите в окно свойств политики.
4. Выберите раздел **Профили политики** в окне свойств политики.
5. Выберите профиль политики, для которого нужно создать правило активации, и нажмите на кнопку **Свойства**.

   В результате откроется окно свойств профиля политики.

   Если список профилей политики пуст, вы можете создать профиль политики (см. стр. 439).
6. Выберите раздел **Правила активации** и нажмите на кнопку **Добавить**.

   В результате запустится мастер создания правила активации профиля политики.
7. В окне **Правила активации профиля политики** установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   - **Общие правила активации профиля политики**

     Установите флажок, чтобы настроить правила активации профиля политики на

устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

- **Правила использования Active Directory**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

- **Правила для определенного владельца устройства**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от того, кто является владельцем устройства, и от членства устройства во внутренней группе безопасности Kaspersky Security Center.

- **Правило для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

8. В окне **Общие условия** настройте следующие параметры:

   - В поле **Устройство в автономном режиме** в раскрывающемся списке укажите условие нахождения устройства в сети:

     - **Да**

       Устройство находится во внешней сети, то есть Сервер администрирования недоступен.

     - **Нет**

       Устройство находится в сети, Сервер администрирования доступен.

     - **Значение не выбрано**

       Критерий не применяется.

   - В поле **Устройство находится в указанном сетевом местоположении** с помощью раскрывающихся списков настройте активацию профиля политики при выполнении / невыполнении на устройстве правила подключения к Серверу администрирования:

     - **Выполняется / Не выполняется**

       Условие активации профиля политики (правило выполняется или не выполняется).

     - **Имя правила**

       Описание сетевого местоположения устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

       Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

   Окно **Общие условия** отображается, если был установлен флажок **Общие правила активации профиля политики**.

9. В окне **Условия с использованием тегов** настройте следующие параметры:

   - Список тегов

     В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

     Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

     В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

   - **Применять к устройствам без выбранных тегов**

     Включите параметр, если необходимо инвертировать выбор тегов.

     Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

     По умолчанию параметр выключен.

   Окно **Условия с использованием тегов** отображается, если был установлен флажок **Общие правила активации профиля политики**.

10. В окне **Условия с использованием Active Directory** настройте следующие параметры:

    - **Членство владельца устройства в группе безопасности Active Directory**

      Если параметр включен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

    - **Членство устройства в группе безопасности Active Directory**

Если параметр включен, профиль политики активируется на устройстве. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Размещение устройства в подразделении Active Directory**

  Если параметр включен, профиль политики активируется на устройстве входит в указанное подразделение Active Directory. Если параметр выключен, критерий активации профиля не применяется.

  По умолчанию параметр выключен.

Окно **Условия с использованием Active Directory** отображается, если был установлен флажок **Правила для использования Active Directory**.

1. В окне **Условия с использованием владельца устройства** настройте следующие параметры:

   - **Владелец устройства**

     Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");
- устройство не принадлежит указанному владельцу (знак "#").

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Владелец устройства входит во внутреннюю группу безопасности**

  Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Активировать профиль политики по наличию роли у владельца устройства**

Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли (см. стр. 771) у его владельца. Добавить роль вручную из списка существующих ролей.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

Окно **Условия с использованием владельца устройства** отображается, если был установлен флажок **Правила для определенного владельца устройства**.

1. В окне **Условия с использованием характеристик оборудования** настройте следующие параметры:

   - **Объем оперативной памяти (МБ)**

     Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

     - объем оперативной памяти устройства меньше указанного значения (знак "<");
     - объем оперативной памяти устройства больше указанного значения (знак ">").

     Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

   - **Количество логических процессоров**

     Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

     - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
     - количество логических процессоров устройства больше или равно указанному значению (знак ">").

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

Окно **Условия с использованием характеристик оборудования** отображается, если был установлен флажок **Правила для характеристик оборудования**.

2. В окне **Имя правила активации профиля политики** в поле **Имя условия** укажите имя правила.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

## Правила перемещения устройств

Рекомендуется автоматизировать процесс размещения устройств в группах администрирования при помощи *правил перемещения устройств*. Правило перемещения состоит из трех основных частей: имени, условия выполнения (см. стр. 1129) (логического выражения над атрибутами устройства) и целевой группы администрирования. Правило перемещает устройство в целевую группу администрирования, если атрибуты устройства удовлетворяют условию выполнения правила.

Правила перемещения устройств имеют приоритеты. Сервер администрирования проверяет атрибуты устройства на соответствие условию выполнения каждого правила, в порядке убывания приоритета правил. Если атрибуты устройства удовлетворяют условию выполнения правила, то устройство перемещается в целевую группу, и на этом обработка правил для этого устройства прекращается. Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

Правила перемещения устройств могут создаваться неявно. Например, в свойствах пакета или задачи удаленной установки может быть указана группа администрирования, в которую должно попасть устройство после установки на нем Агента администрирования. Также правила перемещения могут быть созданы администратором Kaspersky Security Center в явном виде, в списке правил перемещения. Список расположен в Консоли администрирования в свойствах группы **Нераспределенные устройства**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает только один раз устройства, находящиеся в группе **Нераспределенные устройства**. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу **Нераспределенные устройства**. Это рекомендуемый способ использования правил перемещения.

Можно перемещать устройства, уже размещенные в группах администрирования. Для этого в свойствах правила нужно снять флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

Можно создать правило перемещения, способное многократно действовать на одно и то же устройство.

Настоятельно рекомендуется избегать подхода к работе с управляемыми устройствами, при котором одно и то же устройство многократно перемещается из группы в группу, например, с целью применения к устройству особой политики, запуска специальной групповой задачи, обновления с определенной точки распространения.

Подобные сценарии не поддерживаются, так как они крайне неэффективны по нагрузке на Сервер администрирования и на сетевой трафик. Также эти сценарии противоречат модели работы Kaspersky Security Center (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик (см. стр. 427), задачи для выборок устройств (см. стр. 85), назначать Агенты администрирования согласно методике (см. стр. 658) и так далее.

### См. также:


Сценарий: Обнаружение устройств в сети ..... 324

Основной сценарий установки ..... 92

Создание правил автоматического перемещения устройств в группы администрирования ..... 336


## Копирование правил перемещения устройств

Если вам нужно создать несколько правил перемещения устройств с аналогичными параметрами, вы можете скопировать существующее правило, а затем изменить параметры скопированного правила. Например, это удобно, когда вы должны иметь несколько одинаковых правил перемещения устройств с разными IP-диапазонами и целевыми группами.

► *Чтобы скопировать правило перемещения устройств:*

1. Откройте главное окно программы.
2. В папке **Нераспределенные устройства** нажмите на кнопку **Настроить правила**.

   Откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** выберите правило перемещения устройств, которое вы хотите скопировать.
4. Нажмите на кнопку **Клонировать правило**.

Копия выбранного правила будет добавлена в конец списка.

Новое правило будет создано выключенным. Вы можете выключить или изменить правило в любое время.

kaspersky

## Категоризация программного обеспечения

Основным средством контроля запуска приложений являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для программ, не подпадающих ни под одну KL-категорию (например, для программ, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива программы (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Не создавайте автоматически обновляемые категории программного обеспечения для папок Мои документы, %windir%, %ProgramFiles% и %ProgramFiles(x86)%. Файлы в этих папках часто меняются, что приводит к увеличению нагрузки на Сервер администрирования и к увеличению трафика в сети. Следует создать отдельную папку с коллекцией программного обеспечения и время от времени пополнять ее.

## Необходимые условия для установки программ на устройства организации-клиента

Процесс удаленной установки программ на устройства организации-клиента совпадает с процессом удаленной установки программ внутри организации (см. стр. 359).

Для установки программ на устройства организации-клиента необходимо выполнение следующих условий:

- Перед первой установкой программ на устройства организации-клиента требуется установить на них Агент администрирования.

  При настройке инсталляционного пакета Агента администрирования поставщиком услуг в программе Kaspersky Security Center в окне свойств инсталляционного пакета требуется настроить следующие параметры:

  - В разделе **Подключение** в строке **Адрес Сервера администрирования** требуется указать тот же адрес виртуального Сервера администрирования, что и при локальной установке Агента администрирования на точку распространения.
  - В разделе **Дополнительно** требуется установить флажок **Подключаться к Серверу администрирования через шлюз соединений**. В строке **Адрес шлюза соединений** нужно указать адрес точки распространения. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.
- В качестве способа загрузки инсталляционного пакета Агента администрирования необходимо выбрать **Средствами операционной системы с помощью точек распространения**. Выбор способа загрузки осуществляется следующим образом:

- При установке программ с помощью задач удаленной установки способ загрузки можно выбрать двумя способами:
  - при создании задачи удаленной установки в окне **Параметры**;
  - в окне свойств задачи удаленной установки в разделе **Параметры**.
- При установке программ с помощью мастера удаленной установки способ загрузки можно выбрать в окне мастера **Параметры**.

- Учетная запись, под которой работает точка распространения, должна иметь доступ к ресурсу Admin$ на клиентских устройствах.

## Просмотр и изменение локальных параметров программы

Система администрирования Kaspersky Security Center позволяет удаленно управлять локальными параметрами программ на устройствах через Консоль администрирования.

*Локальные параметры программы* – это параметры программы, индивидуальные для устройства. С помощью Kaspersky Security Center вы можете устанавливать локальные параметры программ для устройств, входящих в группы администрирования.

Подробные описания параметров программ "Лаборатории Касперского" приводятся в Руководствах для этих программ.

► *Чтобы просмотреть или изменить локальные параметры программы:*

1. В рабочей области группы, в которую входит нужное вам устройство, выберите закладку **Устройства**.
2. В окне свойств в разделе **Программы** выберите соответствующую программу.
3. Откройте окно свойств программы двойным щелчком мыши по названию программы или нажатием на кнопку **Свойства**.

В результате откроется окно локальных параметров выбранной программы, которые можно просмотреть и изменить.

Вы можете изменять значения тех параметров, изменение которых не запрещено групповой политикой (параметр не закрыт замком (🔒) в политике).

# Обновление Kaspersky Security Center и управляемых программ

В сертифицированном состоянии не допускается загружать и устанавливать обновления модулей программы. Изменение модулей программы может привести к выходу из безопасного состояния.

В этом разделе описаны шаги, которые необходимо выполнить для обновления Kaspersky Security Center и управляемых программ.

kaspersky

## В этом разделе



# Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, программных модулей и программ "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации (см. стр. 400), вы должны поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и программных модулей "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программы безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

**Предварительные требования**

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, программных модулей и программ "Лаборатории Касперского" вручную (см. стр. 1262) или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты программы безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console (см. стр. 1035).
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. стр. 400).
3. Назначено соответствующее количество точек распространения (см. стр. 167) в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и программ "Лаборатории Касперского" состоит из следующих этапов:

**a. Выбор схемы обновления**

Существует несколько схем (см. стр. 453), которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и программ безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

**b. Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и программных модулей для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

Инструкции:

Консоль администрирования: Создание задачи для загрузки обновлений в хранилище Сервера администрирования (см. стр. 461).

Kaspersky Security Center 14.2 Web Console: Создание задачи для загрузки обновлений в хранилище Сервера администрирования (см. стр. 1244).

**c. Создание задачи загрузки обновлений в хранилища агентов обновлений (если требуется)**

По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. 465).

Kaspersky Security Center 14.2 Web Console: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. 1252).

**d. Настройка точек распространения**

Если в вашей сети назначены точки распространения(см. стр. 481), убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования (см. стр. 750).

**e. Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)**

Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (см. стр. 474) (включена по умолчанию), или используя файлы различий (см. стр. 459). Для каждого сегмента сети вы должны выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем программа безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, установите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее** в свойствах политики Агента администрирования (см. стр. 750).

Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или программных модулей "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкции:

Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского" (см. стр. 459).

Консоль администрирования: Включение и выключение офлайн-модели получения обновлений (см. стр. 476).

Kaspersky Security Center 14.2 Web Console: Включение и выключение офлайн-модели получения обновлений (см. стр. 1261).

**f. Проверка полученных обновлений (если требуется)**

Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center 14.2 Web Console.

Инструкции:

Консоль администрирования: Проверка обновлений (см. стр. 470).

Kaspersky Security Center 14.2 Web Console: Проверка обновлений (см. стр. 1250).

**g. Одобрение и отклонение обновлений программного обеспечения**

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center (см. стр. 476) в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для программы безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств. Обновления для компонентов Kaspersky Security Center не могут быть удалены.

Инструкции:

Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (см. стр. 493).

Kaspersky Security Center 14.2 Web Console: Одобрение и отклонение обновлений программного обеспечения (см. стр. 1259).

**h. Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center**

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center (см. стр. 476) устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если параметр выключен, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

Инструкции:

Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 477)

Kaspersky Security Center 14.2 Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 1256)

i. **Установка обновлений для Сервера администрирования**

Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на закладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** `<имя Сервера>` → **Мониторинг**) или на закладке **Уведомления** в Kaspersky Security Center 14.2 Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

j. **Настройка автоматической установки обновлений для программ безопасности**

Создайте задачу *Обновление* для управляемых программ, чтобы обеспечить своевременное обновление программ, программных модулей и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище** (см. стр. 1112).

Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять программы безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. Вы можете изменить параметры обновления в задаче *Обновление*.

Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

Инструкции:

Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (см. стр. 473)

Kaspersky Security Center 14.2 Web Console: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (см. стр. 1257)

**Результаты**

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных программ "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

## См. также:

Сценарий: Настройка защиты сети .....400

# Об обновлении баз, программных модулей и программ "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вы должны своевременно предоставлять обновления следующего:

- баз и программных модулей "Лаборатории Касперского";

Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и программных модулей "Лаборатории Касперского". Если доступ к серверам через системный DNS

невозможен, программа использует публичные DNS-серверы (см. стр. 871). Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

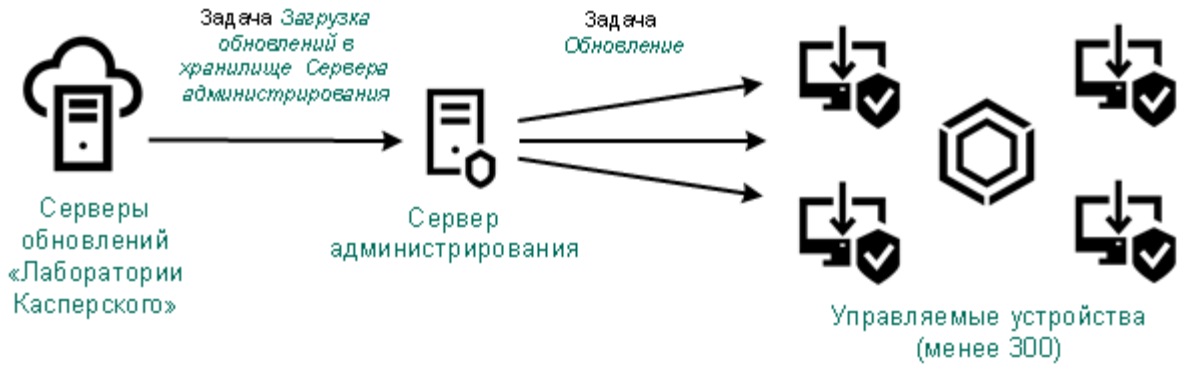
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования.*
- С помощью двух задач:
  - задачи *Загружать обновления в хранилище Сервера администрирования*;
  - задачи *Загружать обновления в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

**Использование задачи Загрузка обновлений в хранилище Сервера администрирования**

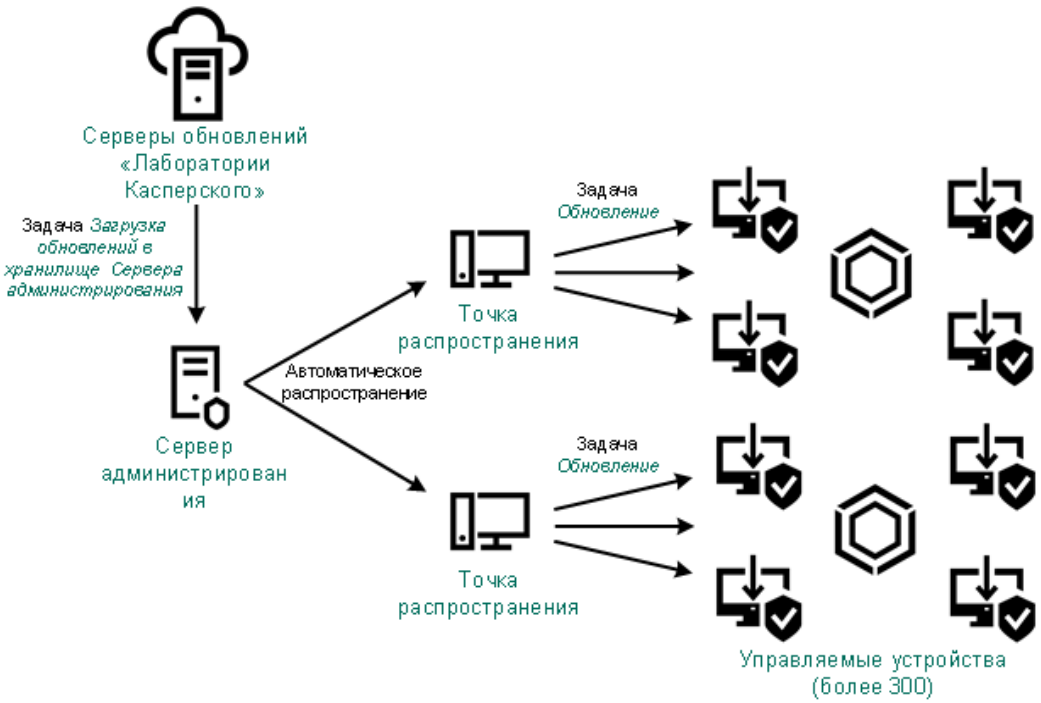
В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загружать обновления в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).




По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения (см. стр. 167) для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать (см. стр. 167) количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.




После завершения задачи *Загружать обновления в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и программные модули "Лаборатории Касперского" для Kaspersky Security Center.

  Эти обновления устанавливаются автоматически.

- Базы и программные модули "Лаборатории Касперского" для программ безопасности на управляемых устройствах.

  Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows (см. стр. 1257).

- Обновления для Сервера администрирования.

  Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

  > Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

  По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования (см. стр. 1256).

- Обновления для программ безопасности.

По умолчанию программа Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. (Вы можете одобрить обновления с помощью Консоли администрирования или  (см. стр. 493) Kaspersky Security Center 14.2 Web Console (см. стр. 1259)). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

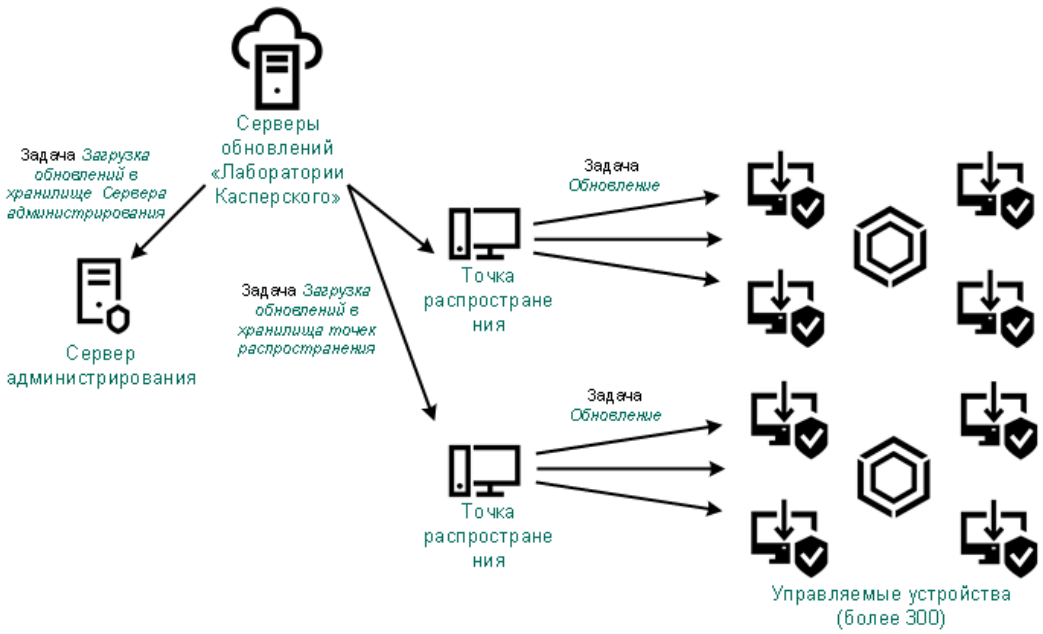
Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются программами. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загружать обновления в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и программных модулей "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия программы;
- идентификатор установки программы;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

**Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения**

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.




По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и / или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загружать обновления в хранилища точек распространения* в дополнение к задаче *Загружать обновления в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

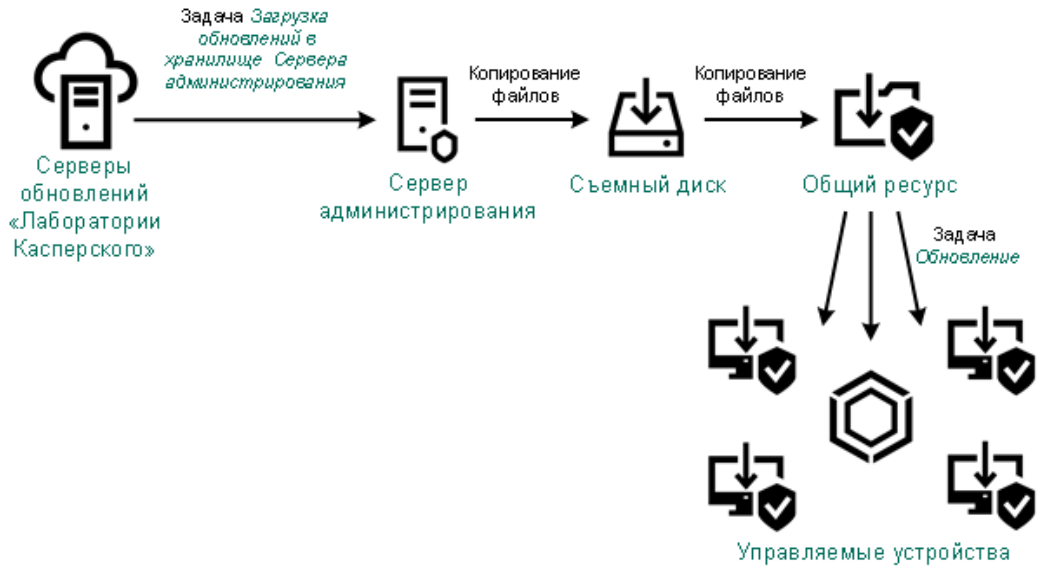
Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Для этой схемы также требуется задача *Загружать обновления в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и программных модулей "Лаборатории Касперского" для Kaspersky Security Center.

**Вручную через локальную папку, общую папку или FTP-сервер**

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, программных модулей и программ "Лаборатории Касперского" (см. стр. 1262). В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную

папку или общий ресурс, указанный в качестве источника обновлений в настройках Kaspersky Endpoint Security (см. рисунок ниже).

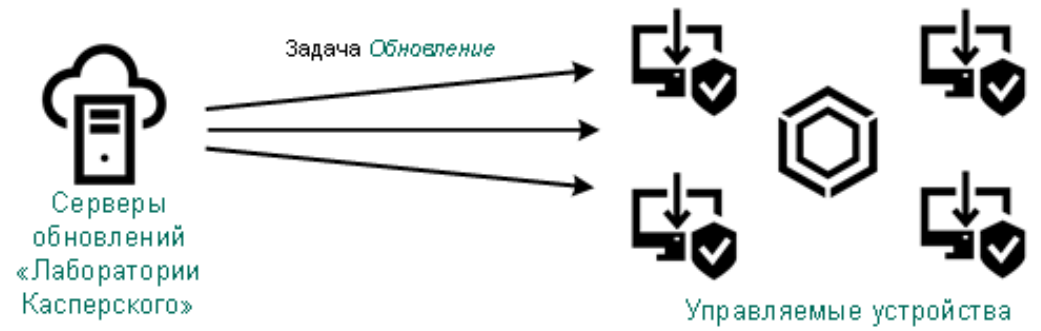



Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих онлайн-справках:

- Онлайн-справка Kaspersky Endpoint Security для Windows.
- Онлайн-справка Kaspersky Endpoint Security для Linux.

**Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах**

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).




В этой схеме программы безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе программы безопасности. Дополнительную информацию об этих параметрах см. в следующих онлайн-справках:

- Онлайн-справка Kaspersky Endpoint Security для Windows.
- Онлайн-справка Kaspersky Endpoint Security для Linux.

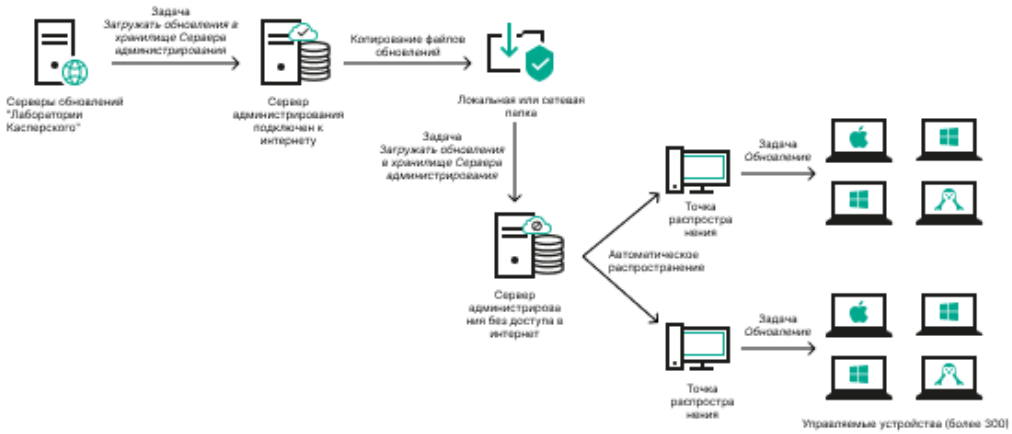
**Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет**

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузить обновления в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются программами безопасности, наборы программ безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 1244), а затем включите параметр **Загружать обновления, используя старую схему**.




- Kaspersky Update Utility https://support.kaspersky.ru/updater4

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера* (см. стр. 1244), а затем включите параметр **Загружать обновления, используя старую схему**.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

# Об использовании файлов различий для обновления баз и программных модулей "Лаборатории Касперского"

Когда Kaspersky Security Center загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

**О функции загрузки файлов различий**

Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий

занимают меньше места, чем целые файлы баз и программных модулей. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и программных модулей.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Функция загрузки файлов различий может быть включена только на Серверах администрирования и точках распространения версии 11 и выше. Чтобы сохранить файлы различий на Серверах администрирования и точках распространения предыдущих версий, их необходимо обновить до версии 11 или выше.
Функция загрузки файлов различий несовместима с офлайн-моделью получения обновлений (см. стр. 474). Это означает, что Агенты администрирования, использующие офлайн-модель загрузки обновлений, не загружают файлы различий, даже если функция загрузки файлов различий включена на Сервере администрирования или точке распространения, которые предоставляют обновления этим Агентам администрирования.
Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Включение функции загрузки файлов различий: сценарий.....460

# Включение функции загрузки файлов различий: сценарий

**Предварительные требования**

Необходимые предварительные условия для сценария:

- Сервер администрирования и точки распространения обновлены до версии 11 или выше.
- Офлайн модель получения обновлений выключена в свойствах политики Агента администрирования.

**Этапы**

a. **Включение функции на Сервере администрирования**

   Включите функцию в свойствах задачи Загрузка обновлений в хранилище Сервера администрирования (см. стр. 927).

b. **Включение функции для точки распространения**

   Включить функцию для точки распространения, которая получает обновления с помощью задачи Загрузка обновлений в хранилища точек распространения

   Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

Эта функция включается в свойствах политики Агента администрирования (см. стр. 750) и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения** (см. стр. 485).

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

### См. также:

Об использовании файлов различий для обновления баз и программных модулей "Лаборатории Касперского" ..... 459

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449

Об обновлении баз, программных модулей и программ "Лаборатории Касперского" ..... 453

## Создание задачи для загрузки обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загрузка обновлений в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

► *Чтобы создать задачу загрузки обновлений в хранилище Сервера администрирования:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню **Задачи** в дереве консоли выберите пункт **Новый → Задача**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать категорию**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите **Загрузка обновлений в хранилище Сервера администрирования**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
   - **Источники обновлений**
   - **Другие параметры**:
     - **Принудительно обновить подчиненные Серверы**

       Если флажок установлен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

       По умолчанию параметр выключен.
     - **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

  Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

  Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

1. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного

времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления

устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилище Сервера администрирования** появится в рабочей области списка задач Сервера администрирования.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

### См. также:

Проверка полученных обновлений ..... 470

Загрузка обновлений в хранилище Сервера администрирования ..... 927

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449

## Создание задачи загрузки обновлений в хранилища точек распространения

Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

► *Чтобы создать задачу загрузки обновлений в хранилища точек распространения для выбранной группы администрирования:*

1. В дереве консоли выберите папку **Задачи**.
2. По кнопке **Создать задачу** в рабочей области папки запустите мастер создания задачи.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Загрузка обновлений в хранилища точек распространения**.

4. В окне мастера **Параметры**, укажите следующие параметры задачи:

- **Источники обновлений**

В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

  По умолчанию этот вариант выбран.

- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует аутентификации, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Загружать обновления, используя старую схему**

1. В окне мастера **Выберите группу администрирования** нажмите на кнопку **Обзор** и выберите группу администрирования, для которой задача будет применена.
2. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты

и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

- антивирусы для рабочих станций и файловых серверов;
- антивирусы защиты периметра;
- антивирусы для почтовых систем.

По умолчанию выбраны все типы программ.

Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера созданная задача **Загрузка обновлений в хранилища точек распространения** появится в списке задач Агента администрирования в соответствующей группе администрирования и в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

В окне свойств Сервера администрирования выберите раздел **Точки распространения**. В свойствах каждой точки распространения в разделе **Источники обновлений** можно указать источники обновлений (**Получать с Сервера администрирования** или **Использовать задачу принудительной загрузки обновлений**). Для точки распространения, назначенной вручную или автоматически, по умолчанию выбран вариант **Получать с Сервера администрирования**. Такие точки распространения будут использовать результаты задачи *Загрузка обновлений в хранилища точек распространения*.

В свойствах каждой точки распространения указана сетевая папка, настроенная индивидуально для этой точки распространения. Названия папок могут быть разными для разных точек распространения. Поэтому не рекомендуется изменять сетевую папку обновлений в свойствах задачи, если задача создается для группы устройств.

Вы можете изменить сетевую папку обновлений в свойствах задачи *Загрузка обновлений в хранилища точек распространения*, если вы создаете локальную задачу для устройства.

### См. также:

Параметры задачи загрузки обновлений в хранилища точек распространения .....929

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Настройка параметров задачи загрузки обновлений в хранилище Сервера администрирования

► *Чтобы настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования:*

1. В рабочей области папки дерева консоли **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования** в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:

- В контекстном меню файла выберите пункт **Свойства**.
- По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.

Откроется окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*. В нем вы можете настроить параметры загрузки обновлений в хранилище Сервера администрирования.

См. также:

Загрузка обновлений в хранилище Сервера администрирования .....927

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования (<Папка установки Kaspersky Security Center>\Share\Updates). Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загружать обновления в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты программы безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования (см. стр. 709) с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи *Обновление* и *Поиск вредоносного ПО* (см. стр. 1111) для программы, поддерживаемой Kaspersky Security Center, например, Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server. При создании задач *Обновление* и *Поиск вредоносного ПО* укажите группу администрирования с тестовыми устройствами.

   Задача *Проверка обновлений* последовательно запускает задачи *Обновление* и *Поиск вредоносного ПО* на тестовых устройствах и так проверяет, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи *Обновление* и *Поиск вредоносного ПО*.

3. Использование задачи *Загружать обновления в хранилище Сервера администрирования*(см. стр. 461).

► *Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:*

1. В рабочей области папки **Задачи** дерева консоли выберите задачу *Загрузка обновлений в хранилище Сервера администрирования* в списке задач.
2. Откройте окно свойств задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Настроить параметры задачи** в блоке работы с выбранной задачей.
3. Если задача *Проверка обновлений* существует, нажмите на кнопку **Обзор**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.
4. Если вы не создали задачу *Проверка обновлений* ранее, нажмите на кнопку **Создать**.

   В результате запустится мастер создания задачи проверки обновлений. Следуйте далее указаниям мастера.
5. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **ОК**.

Автоматическая проверка обновлений включена. Теперь можно запустить задачу *Загружать обновления в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Настройка проверочных политик и вспомогательных задач

При создании задачи *Проверки обновлений* (см. стр. 470) Сервер администрирования формирует проверочные политики, а также вспомогательные групповые задачи обновления и проверки по требованию.

На выполнение вспомогательных групповых задач обновления и проверки по требованию требуется некоторое время. Эти задачи выполняются в рамках выполнения задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется в рамках выполнения задачи *Загрузка обновлений в хранилище*. Время выполнения задачи *Загрузки обновлений в хранилище* включает в себя время выполнения вспомогательных групповых задач обновления и проверки по требованию.

Параметры проверочных политик и вспомогательных задач можно изменять.

► *Чтобы изменить параметры проверочной политики или вспомогательной задачи:*

1. В дереве консоли выберите группу, для которой сформирована задача *Проверка обновлений*.
2. В рабочей области группы выберите одну из следующих закладок:
   - **Политики**, если вы хотите изменить параметры проверочной политики.
   - **Задачи**, если вы хотите изменить параметры вспомогательной задачи.
3. В рабочей области закладки выберите политику или задачу, параметры которой вы хотите изменить.
4. Откройте окно свойств этой политики (задачи) одним из следующих способов:
   - В контекстном меню политики (задачи) выберите пункт **Свойства**.
   - По ссылке **Настроить параметры политики** (**Настроить параметры задачи**) в блоке работы с выбранной политикой (задачей).

Чтобы проверка обновлений выполнялась правильно, необходимо соблюдать следующие ограничения на изменение параметров проверочных политик и вспомогательных задач:

- В параметрах вспомогательных задач:
  - Сохранять на Сервере администрирования все события с уровнями важности **Критическое событие** и **Отказ функционирования**. На основе событий этих типов Сервер администрирования проводит анализ работы программ.
  - Использовать в качестве источника обновлений Сервер администрирования.
  - Указывать тип расписания задач: **Вручную**.
- В параметрах проверочных политик:
  - Отключить технологии проверки iChecker и iSwift (**Базовая защита → Защита от файловых угроз → Параметры → Дополнительно → Технологии проверки**).
  - Выбрать действия над зараженными объектами: **Лечить; удалять, если лечение невозможно** / **Лечить; блокировать, если лечение невозможно** / **Блокировать**. (**Базовая защита → Защита от файловых угроз → Действие при обнаружении угрозы**).
- В параметрах проверочных политик и вспомогательных задач:

  Если после установки обновлений программных модулей потребуется перезагрузка устройства, ее следует выполнить незамедлительно. Если устройство не будет перезагружено, то проверить этот тип обновлений будет невозможно. Для некоторых программ установка обновлений, требующих перезагрузки, может быть запрещена или выполняться только после подтверждения от пользователя. Эти ограничения должны быть отключены в параметрах проверочных политик и вспомогательных задач.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Просмотр полученных обновлений

► *Чтобы просмотреть список полученных обновлений,*

в дереве консоли в папке **Хранилища** выберите вложенную папку **Обновления и патчи ПО "Лаборатории Касперского"**.

В рабочей области папки **Обновления и патчи ПО "Лаборатории Касперского"** представлен список обновлений, сохраненных на Сервере администрирования.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства

Вы можете настроить автоматическое обновление баз и модулей программы Kaspersky Endpoint Security на клиентских устройствах.

► *Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security на устройства:*

1. В дереве консоли выберите папку **Задачи**.
2. Создайте задачу с типом **Обновление** одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Новый → Задача**.
   - В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Обновление**.
4. Следуйте дальнейшим шагам мастера.

   В результате работы мастера создается задача обновления для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.
5. В рабочей области папки **Задачи** выберите созданную задачу обновления.
6. В контекстном меню задачи выберите пункт **Свойства**.
7. В открывшемся окне свойств задачи выберите раздел **Свойства**.

   В разделе **Свойства** можно настроить параметры задачи обновления в локальном и мобильном режимах:
   - **Параметры обновления в локальном режиме**: между устройством и Сервером администрирования установлена связь.
   - **Параметры обновления в мобильном режиме**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).
8. По кнопке **Параметры** выберите источник обновлений.
9. Выберите параметр **Загружать обновления модулей программы**, чтобы одновременно с базами программы загружать и устанавливать обновления модулей программы.

   Если флажок установлен, то Kaspersky Endpoint Security уведомляет пользователя о доступных обновлениях модулей программы и во время выполнения задачи обновления включает обновления модулей программы в пакет обновлений. Настройте применение модулей обновлений:
   - **Устанавливать критические и одобренные обновления**. При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает обновления со статусом *Предельный*

автоматически; остальные обновления модулей программы – после одобрения их установки администратором.

- **Устанавливать только утвержденные обновления**. При наличии обновлений модулей программы Kaspersky Endpoint Security устанавливает их после одобрения их установки, локально через интерфейс программы или с помощью Kaspersky Security Center.

Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то программа устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

10. Выберите параметр **Копировать обновления в папку**, чтобы программа сохраняла загруженные обновления в папку, указанную по кнопке **Обзор**.
11. Нажмите на кнопку **ОК**.

При выполнении задачи **Обновление** программа отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых программ.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Офлайн-модель получения обновлений

Установка обновлений исполняемых модулей программ «Лаборатории Касперского», не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программ из безопасного состояния.

Агент администрирования на управляемых устройствах не всегда может подключиться к Серверу администрирования для получения обновлений. Например, Агент администрирования может быть установлен на ноутбук, который иногда не подключен к интернету и локальной сети. Также администратор может ограничить время подключения устройств к сети. В таких случаях устройства с установленным Агентом администрирования не смогут получить обновления от Сервера администрирования в соответствии с расписанием. Если настроено обновление управляемых программ (например, Kaspersky Endpoint Security) с помощью Агента администрирования, для обновления требуется соединение с Сервером администрирования. Когда соединение между Агентом администрирования и Сервером администрирования отсутствует, обновление невозможно. Соединение Агента администрирования с Сервером может быть настроено так, чтобы Агент подключался к Серверу только в определенные периоды времени. В худшем случае, если настроенные периоды подключения "пересекаются" с периодами, когда связь отсутствует, базы никогда не будут обновлены. Также возможны ситуации, когда много управляемых программ одновременно обращаются к Серверу администрирования за обновлениями. В этом случае Сервер администрирования может перестать отвечать на запросы (как во время DDoS-атаки).

Во избежание описанных проблем в Kaspersky Security Center реализована офлайн-модель получения обновления баз и модулей управляемых программ. Эта модель обеспечивает надежность механизма распространения обновлений вне зависимости от временных проблем недоступности каналов связи сервера администрирования, а также снижает нагрузку на Сервер администрирования. Эта модель также снижает нагрузку на Сервер администрирования.

**Как работает офлайн-модель получения обновлений**

Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых программ. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для программ на клиентских устройствах, но подключение не требуется для обновления.

Чтобы распределить нагрузку на Сервер администрирования, Агент администрирования на устройстве подключается к Серверу и загружает обновления случайным образом в течение интервала времени, определенного Сервером. Интервал времени зависит от количества устройств с установленным Агентом администрирования, которые загружают обновления, и от размера обновлений. Для снижения нагрузки на Сервер администрирования вы можете использовать Агент администрирования в качестве точки распространения.

Если офлайн-модель получения обновлений отключена, обновления распространяются в соответствии с расписанием задачи загрузки обновлений в хранилище.

По умолчанию офлайн-модель получения обновлений включена.

Офлайн-модель получения обновлений используется только для тех управляемых устройств, на которых задача получения обновлений управляемыми программами имеет расписание **При загрузке обновлений в хранилище**. Для остальных управляемых устройств используется традиционная система получения обновлений с Сервера администрирования в реальном времени.

Рекомендуется выключить офлайн-модель получения обновлений через настройки политик Агента администрирования соответствующих групп администрирования, если в управляемых программах настроено получение обновлений не с Сервера администрирования, а с серверов "Лаборатории Касперского" либо из сетевой папки и при этом задача получения обновлений имеет расписание **При загрузке обновлений в хранилище**.

## См. также:

Включение и выключение офлайн-модели получения обновлений .....476

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам снять флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для программ "Лаборатории Касперского" настроена.

► *Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

   По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

### См. также:

Офлайн-модель получения обновлений ..... 474

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449

## Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center

Установка обновлений исполняемых программных модулей программ «Лаборатории Касперского», не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программ из безопасного состояния.

По умолчанию автоматически устанавливаются загруженные обновления и патчи для следующих компонентов программы:

- Агент администрирования для Windows;
- Консоль администрирования;
- Сервер мобильных устройств Exchange ActiveSync;

- Сервер iOS MDM.

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center доступна только для устройств под управлением Windows. Вы можете выключить автоматическую установку обновлений и патчей для этих компонентов. В этом случае загруженные обновления и патчи будут установлены только после того, как вы измените их статус на *Одобрено*. Обновления и патчи со статусом *Не определено* не будут установлены.

### См. также:

Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center ..... 477

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449

## Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство:*

1. Запустите локальную установку Агента администрирования на устройство (см. стр. 205).
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета:*

1. В дереве консоли выберите папку **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню пакета **Агент администрирования Kaspersky Security Center <номер версии>** выберите пункт **Свойства**.
3. В свойствах инсталляционного пакета в разделе **Параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

► *Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить или выключить автоматическую установку обновлений и патчей.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики выберите раздел **Управление патчами и обновлениями**.
6. Установите или снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**, чтобы соответственно включить или выключить автоматическую установку.
7. Установите замок при этом флажке.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

### См. также:


Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center .....476

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449


## Автоматическое распространение обновлений

Kaspersky Security Center позволяет автоматически распространять и устанавливать обновления на клиентские устройства и подчиненные Серверы администрирования.

### См. также:


Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449


### В этом разделе

## Автоматическое распространение обновлений на клиентские устройства

► *Чтобы обновления выбранной вами программы автоматически распространялись на клиентские устройства сразу после загрузки обновлений в хранилище Сервера администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся клиентские устройства.
2. Создайте задачу распространения обновлений этой программы для выбранных клиентских устройств одним из следующих способов:
   - Если требуется распространять обновления на клиентские устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. стр. 413).
   - Если требуется распространять обновления на клиентские устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. стр. 415).

   Запустится мастер создания задачи. Следуйте его указаниям, выполнив следующие условия:

   a. В окне мастера **Тип задачи** в узле нужной вам программы выберите задачу распространения обновлений.

   > Название задачи распространения обновлений, которое отображается в окне **Тип задачи**, зависит от программы, для которой создается задача. Подробнее о названиях задач обновления для выбранных программ "Лаборатории Касперского" см. в Руководствах к этим программам.

   b. В окне мастера **Расписание** в поле **Запуск по расписанию** выберите вариант запуска **При загрузке обновлений в хранилище**.

В результате созданная задача распространения обновлений будет запускаться для выбранных устройств каждый раз при загрузке обновлений в хранилище Сервера администрирования.

Если задача распространения обновлений нужной вам программы уже создана для выбранных устройств, для автоматического распространения обновлений на клиентские устройства в окне свойств задачи в разделе **Расписание** нужно выбрать вариант запуска **При загрузке обновлений в хранилище** в поле **Запуск по расписанию**.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Автоматическое распространение обновлений на подчиненные Серверы администрирования

► *Чтобы обновления выбранной вами программы автоматически распространялись на подчиненные Серверы администрирования сразу после загрузки обновлений в хранилище главного Сервера администрирования:*

1. В дереве консоли в узле главного Сервера администрирования выберите папку **Задачи**.
2. В списке задач в рабочей области выберите задачу загрузки обновлений в хранилище Сервера администрирования.

3. Откройте раздел **Параметры** окна свойств выбранной задачи одним из следующих способов:
   - В контекстном меню файла выберите пункт **Свойства**.
   - По ссылке **Изменить параметры** в блоке работы с выбранной задачей.
4. В разделе **Параметры** окна свойств задачи откройте окно **Прочие параметры** по ссылке **Настроить** в подразделе Прочие параметры.
5. В открывшемся окне **Прочие параметры** установите флажок **Принудительно обновить подчиненные Серверы**.

В параметрах задачи получения обновлений Сервером администрирования на закладке **Параметры** окна свойств задачи установите флажок **Принудительно обновить подчиненные Серверы**.

В результате сразу после получения обновлений главным Сервером администрирования будут автоматически запускаться задачи загрузки обновлений подчиненными Серверами администрирования, независимо от расписания, установленного в параметрах этих задач.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

► *Чтобы назначить точки распространения автоматически:*

1. Откройте главное окно программы.
2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распределения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

kaspersky

## Назначение устройства точкой распространения вручную

Kaspersky Security Center позволяет назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию (см. стр. 167).

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

► *Чтобы вручную назначить устройство точкой распространения:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** нажмите на кнопку **Добавить**. Кнопка доступна, если выбран вариант **Вручную назначать точки распространения**.

   Откроется окно **Добавление точки распространения**.
4. В окне **Добавление точки распространения** выполните следующие действия:
   a. Выберите устройство, которое будет выполнять роль точки распространения (в группе администрирования или укажите IP-адрес устройства). При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения (см. стр. 88).
   b. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.
5. Нажмите на кнопку **ОК**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.
6. Выберите в списке добавленную точку распространения и по кнопке **Свойства** откройте окно ее свойств.
7. В окне свойств настройте параметры точки распространения:
   - В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.
     - **Номер SSL-порта**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.
     - **Использовать многоадресную IP-рассылку**

       Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

       Многоадресная IP-рассылка уменьшает время, необходимое для установки программ из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке программы на одно клиентское

устройство.

- **Адрес многоадресной IP-рассылки**

  IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

  По умолчанию Kaspersky Security Center автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

- **Номер порта IP-рассылки**

  Номер порта многоадресной рассылки.

  Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Распространять обновления**

  Обновления распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить (см. стр. 167) количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок обновлений и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Распространять инсталляционные пакеты**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить (см. стр. 167) количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- Использовать точку распространения в качестве извещающего сервера
- Порт push-сервера

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и / или сетевое местоположение).

- В разделе **Прокси-сервер KSN** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.
  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

    Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены (см. стр. 830) в окне свойств Сервера администрирования.

    Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.
  - **Переслать KSN запрос Серверу администрирования**

    Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

    По умолчанию параметр включен.
  - **Доступ к облачной-службе KSN / Локальному KSN непосредственно через интернет**

    Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или Локальному KSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или Локальный KSN.

    Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к Локальному KSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения.

    Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к Локальному KSN.
  - **Игнорировать параметры прокси-сервера для подключения к Локальному KSN**

    Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали Локальный KSN напрямую. В противном случае запрос от управляемой программы не будет передан в Локальный KSN.

    Это параметр доступен, если вы выбрали параметр **Доступ к облачной-службе KSN/Локальному KSN непосредственно через интернет**.
  - **TCP-порт**

    Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.
  - **UDP-порт**

Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- В разделе **Обнаружение устройств** настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения.
  - **Windows-домены**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.
  - **Active Directory**

    Вы можете включить опрос Active Directory и задать расписание опроса.

    Если вы установили флажок **Разрешить опрос Active Directory**, выберите один из следующих вариантов:

    - **Опросить текущий домен Active Directory**.
    - **Опросить лес доменов Active Directory**.
    - **Опросить указанные домены Active Directory**. Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.
  - **IP-диапазоны**

    Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

    Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов (см. стр. 667).

    Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вы должны установить утилиту avahi-browse на точке распространения.
- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.
  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.
  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

В результате выбранные устройства будут выполнять роль точек распространения.

Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Удаление устройства из списка точек распространения

► *Чтобы удалить устройство из списка точек распространения:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите устройство, выполняющее функции точки распространения, и нажмите на кнопку **Удалить**.

В результате устройство будет удалено из списка точек распространения и перестанет выполнять функции точки распространения.

Нельзя удалить устройство из списка точек распространения, если оно было назначено Сервером администрирования автоматически (см. стр. 481).

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Загрузка обновлений точками распространения

Kaspersky Security Center позволяет точкам распространения получать обновления от Сервера администрирования, серверов "Лаборатории Касперского", из локальной или сетевой папки.

► *Чтобы настроить получение обновлений для точки распространения:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Точки распространения** выберите точку распространения, через которую обновления будут доставляться на клиентские устройства группы.
4. По кнопке **Свойства** откройте окно свойств выбранной точки распространения.
5. В окне свойств точки распространения выберите раздел **Источник обновлений**.
6. Выберите источник обновлений для точки распространения:
   - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получать с Сервера администрирования**:

- **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. стр. 459).

По умолчанию параметр включен.

- Чтобы точка распространения получала обновления с помощью задачи, выберите вариант **Использовать задачу принудительной загрузки обновлений**:
  - Нажмите на кнопку **Выбрать**, если такая задача уже есть на устройстве, и выберите задачу в появившемся списке.
  - Нажмите на кнопку **Новая задача**, чтобы создать задачу, если такой задачи еще нет на устройстве. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  Задача загрузки обновлений в хранилища точек распространения является локальной. Для каждого устройства, выполняющего роль точки распространения, задачу требуется создавать отдельно.

В результате точка распространения будет получать обновления из указанного источника.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Удаление обновлений программного обеспечения из хранилища

► *Чтобы удалить обновления программного обеспечения из хранилища Сервера администрирования:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** выберите обновление, которое нужно удалить.
3. В контекстном меню обновления выберите **Удалить файлы обновлений**.

Обновления программного обеспечения будут удалены из хранилища Сервера администрирования.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Установка патча для программы "Лаборатории Касперского" в кластерной модели

Kaspersky Security Center поддерживает только ручную установку патчей для программ "Лаборатории Касперского" в кластерной модели.

► *Чтобы установить патч для программы "Лаборатории Касперского":*

1. Загрузите на каждый узел кластера патч.

2. Запустите установку патча на активном узле.
3. Дождитесь успешной установки патча.
4. Последовательно запустите патч на всех подчиненных узлах кластера.

   При запуске патча из командной строки используйте ключ "`-CLUSTER_SECONDARY_NODE`".

   В результате этих действий патч будет установлен на каждом узле кластера.
5. Запустите вручную кластерные службы "Лаборатории Касперского".

Каждый узел кластера будет отображаться в Консоли администрирования как устройство с установленным Агентом администрирования.

Информацию об установленных патчах можно просмотреть в папке **Обновления программного обеспечения** или в отчете о версиях обновлений программных модулей программ "Лаборатории Касперского".

### См. также:


Настройка общих параметров Сервера администрирования ..... 685

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449


# Управление программами сторонних производителей на клиентских устройствах

Kaspersky Security Center позволяет управлять программами "Лаборатории Касперского" и других производителей, установленными на клиентских устройствах.

Администратор может выполнять следующие действия:

- создавать категории программ на основании заданных критериев;
- управлять категориями программ с помощью специально созданных правил;
- управлять запуском программ на устройствах;
- выполнять инвентаризацию и вести реестр программного обеспечения, установленного на устройствах;
- закрывать уязвимости программного обеспечения, установленного на устройствах;
- устанавливать обновления Windows Update и других производителей программного обеспечения на устройствах;
- отслеживать использование лицензионных ключей для групп лицензионных программ.

### В этом разделе


Установка обновлений программ сторонних производителей ..... 488

Уязвимости в программах ..... 515

Группы программ ..... 554

kaspersky

# Установка обновлений программ сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения, установленного на клиентских устройствах, и закрывать уязвимости в программах Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи поиска обновлений и загружает обновления в хранилище обновлений. После завершения поиска обновлений программа предоставляет администратору информацию о доступных обновлениях и об уязвимостях в программах, которые можно закрыть с помощью этих обновлений.

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Для использования Сервера администрирования в роли сервера Windows Update необходимо настроить синхронизацию обновлений с центром обновлений Windows. После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

Управлять обновлениями программного обеспечения можно также с помощью политики Агента администрирования. Для этого необходимо создать политику Агента администрирования и настроить параметры обновлений программного обеспечения в соответствующих окнах мастера создания политики.

Администратор может просматривать список доступных обновлений в папке **Обновления программного обеспечения**, входящей в состав папки **Управление программами**. Эта папка содержит список полученных Сервером администрирования обновлений программ Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства. После просмотра информации о доступных обновлениях администратор может выполнить установку обновлений на устройства.

Обновление некоторых программ Kaspersky Security Center выполняет путем удаления предыдущей версии программы и установки новой версии.
Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.
Убедитесь, что параметр **Отображать Системное администрирование** включен в окне **Настройка интерфейса** для главного и подчиненного Серверов администрирования (см. стр. 322). В противном случае задача поиска обновлений обрабатывает только обновления WSUS.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений программ сторонних производителей, которые можно установить с помощью Системного администрирования. Кроме того, специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях, и не проводят другие виды анализа упомянутых выше обновлений.

Перед установкой обновлений на все устройства можно выполнить проверочную установку, чтобы убедиться, что установленные обновления не вызовут сбоев в работе программ на устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе Управление Сервером (https://support.kaspersky.ru/14758).

## В этом разделе



## Сценарий: Обновление программ сторонних производителей

В этом разделе представлен сценарий обновления программ сторонних производителей, установленных на клиентских устройствах. Программы сторонних производителей включают в себя программы от Microsoft и других поставщиков программного обеспечения (см. стр. 1275). Обновления для программ Microsoft предоставляются службой Центра обновления Windows.

### Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений программ сторонних производителей, отличных от программ Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений программ Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления программ Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

### Этапы

Обновление производителей состоит из следующих этапов:

**a. Поиск требуемых обновлений**

Чтобы найти обновления программ сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в программах (см. стр. 522), Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).

- Kaspersky Security Center 14.2 Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (см. стр. 1289), параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

**b. Анализ списка найденных обновлений**

Просмотрите список **Обновление программного обеспечения** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации о доступных обновлениях (см. стр. 492).
- Kaspersky Security Center 14.2 Web Console: Просмотр информации о доступных обновлениях программ сторонних производителей (см. стр. 1305).

**c. Настройка установки обновлений**

После того как Kaspersky Security Center получает список обновлений программ сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Создайте одну из этих задач. Вы можете создать эти задачи на закладке **Задачи** или с помощью списка **Обновление программного обеспечения**.

Задача *Установка требуемых обновлений и закрытия уязвимостей* используется для установки обновлений для программ Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления программ других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вы должны принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в программах (см. стр. 527), Просмотр информации о доступных обновлениях (см. стр. 492).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295), Создание задачи Установка обновлений Центра обновления Windows (см. стр. 1303), Просмотр информации о доступных обновлениях программ сторонних производителей (см. стр. 1305).

**d. Задание расписания задачи**

Чтобы убедится, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При планировании задачи *Установка обновлений Центра обновления*

*Windows* обратите внимание, что для этой задачи вы должны определять список обновлений каждый раз перед запуском этой задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

**e. Одобрение и отклонение обновлений программного обеспечения (если требуется)**

Если вы создали задачу Установка требуемых обновлений и закрытие уязвимостей, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу Установка обновлений Центра обновления Windows, пропустите этот шаг.

Для каждого правила вы можете определить обновления для установки в зависимости от статуса обновления: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения** (**Операции** → **Управление патчами** → **Обновления программного обеспечения**).

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (см. стр. 493).
- Kaspersky Security Center 14.2 Web Console: Одобрение и отклонение обновлений программ сторонних производителей (см. стр. 1308).

**f. Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)**

По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизовано службам Центра обновления Windows на сетевых устройствах.

Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Инструкции:

- Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования (см. стр. 494), Настройка обновлений Windows в политике Агента администрирования (см. стр. 513).

- Kaspersky Security Center 14.2 Web Console: Создание задачи Синхронизация обновлений Windows Update (см. стр. 1309).

**g. Запуск задачи установки обновлений**

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

**h. Создание отчета о результатах установки обновлений программ сторонних производителей (если требуется)**

Для просмотра статистики установки обновлений создайте **Отчет о результатах установки обновлений стороннего ПО**.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (см. стр. 588).
- Kaspersky Security Center 14.2 Web Console: Генерация и просмотр отчета (см. стр. 1372).

**Результаты**

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

## См. также



# Просмотр информации о доступных обновлениях для программ сторонних производителей

► *Чтобы просмотреть список доступных обновлений для программ сторонних производителей, установленных на клиентских устройствах,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.

В рабочей области папки вы можете просматривать список имеющихся обновлений для программ, установленных на устройствах.

► *Чтобы просмотреть свойства обновления,*

В рабочей области папки **Обновления программного обеспечения** в контекстном меню обновления выберите пункт **Свойства**.

В окне свойств обновления для просмотра доступна следующая информация:

- В разделе **Общие** можно просмотреть **Статус одобрения обновления**:
  - **Не определено** – обновление доступно в списке обновлений, но не одобрено для установки.
  - **Одобрено** – обновление доступно в списке обновлений и одобрено к установке.
  - **Отклонено** – обновление отклонено для установки.
- В разделе **Атрибуты** вы можете просмотреть значения поля **Устанавливаемый автоматически**:
  - Значение **Автоматически** отображается, если задача *Установка требуемых обновлений и закрытие уязвимостей* может устанавливать обновления для программы. Задача автоматически устанавливает новые обновления с веб-адреса, предоставленного поставщиком программ сторонних производителей.
  - Значение **Вручную** отображается, если Kaspersky Security Center не может установить обновления для программы автоматически. Вы можете установить обновления вручную.

  Поле **Устанавливаемый автоматически** не отображается для обновлений программ Windows.
- Список клиентских устройств, для которых применимо обновление.
- Список системных компонентов (предварительных требований), которые должны быть установлены перед обновлением (любым).
- Уязвимости в программах, которые закрывают это обновление.

## См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

## Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Для управления установкой обновлений программ сторонних производителей использование статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений программ сторонних производителей, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В дереве консоли выберите узел **Дополнительно → Управление программами → Обновления программного обеспечения**.
2. В рабочей области папки **Обновления программного обеспечения** перейдите по ссылке **Обновить** вверху справа и дождитесь загрузки списка обновлений. Отобразится список обновлений.
3. Выберите обновления, которые требуется подтвердить или отклонить.

   Блок работы с выбранным объектом отображается в правой части рабочей области.
4. В раскрывающемся списке **Одобрение обновления** выберите **Одобрено**, чтобы подтвердить выбранные обновления, или **Отклонено**, чтобы отменить выбранные обновления.

   По умолчанию установлено значение **Не определено**.

Обновления, для которых установлен статус **Одобрено**, помещаются в очередь на установку.

Обновления, для которых установлен статус **Отклонено**, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для программ "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус **Отклонено**, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем. Если обновления для программ "Лаборатории Касперского" не могут быть удалены, это отображается в окне свойств обновления: в разделе **Общие** и в разделе **Требования при установке**. Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Сценарий:Обновление программ сторонних производителей.....489

## Синхронизация обновлений Windows Update с Сервером администрирования

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Использовать Сервер администрирования в роли WSUS-сервера**, задача синхронизации обновлений Windows Update создается автоматически. Запустить задачу можно в папке **Задачи**. Функция обновления программного обеспечения Microsoft доступна только после успешного завершения задачи **Синхронизация обновлений Windows Update**.

Обновления программного обеспечения Microsoft могут превышать 10 ГБ. Убедитесь, что база данных Сервера администрирования способна вместить такие тома, иначе задача **Синхронизация обновлений Windows Update** не будет выполнена. База данных Microsoft SQL Express не поддерживается для задачи **Синхронизация обновлений Windows Update**.

Задача **Синхронизация обновлений Windows Update** загружает с серверов Microsoft только метаданные. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы создать задачу синхронизации обновлений Windows Update с Сервером администрирования:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить синхронизацию обновлений Windows Update**.

   В результате работы мастера создается задача **Синхронизация обновлений Windows Update**, которая отображается в папке **Задачи**.

   Запустится мастер создания задачи получения данных из центра обновлений Windows. Следуйте далее указаниям мастера.

Задачу синхронизации обновлений Windows Update также можно создать в папке **Задачи** по кнопке **Создать задачу**.

Microsoft периодически удаляет со своих серверов устаревшие обновления, так что число актуальных обновлений составляет от 200 000 до 300 000. Для уменьшения используемого дискового пространства и размера базы данных, Kaspersky Security Center реализовано удаление устаревших обновлений, которые отсутствуют на серверах обновлений Microsoft.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, программа получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание базы данных** (см. стр. 870) можно удалить такие устаревшие записи из базы данных и соответствующих им файлов.

kaspersky

## См. также:



## В этом разделе



## Шаг 1. Определение необходимости уменьшения трафика

Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, вы можете выключить параметр **Загружать файлы экспресс-установки**.

Если параметр выбран, в процессе выполнения задачи загружаются файлы экспресс-установки. По умолчанию вариант не выбран.

## См. также:



## Шаг 2. Программы

В этом разделе можно выбрать программы, для которых будут загружаться обновления.

Если установлен флажок **Все программы**, то обновления будут загружаться для всех имеющихся программ, а также для тех программ, которые могут быть выпущены в будущем.

По умолчанию флажок **Все программы** установлен.

## См. также:

## Шаг 3. Категории обновлений

В этом разделе можно выбрать категории обновлений, которые будут загружаться на Сервер администрирования.

Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.

По умолчанию флажок **Все категории** установлен.

### См. также:

Синхронизация обновлений Windows Update с Сервером администрирования ..... 494

Сценарий:Обновление программ сторонних производителей ..... 489

## Шаг 4. Языки локализации обновлений

В этом окне можно выбрать языки локализации обновлений, которые будут загружаться на Сервер администрирования. Выберите один из следующих вариантов загрузки языков локализации обновлений:

- **Загружать все языки, включая новые**

  Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

- **Загружать выбранные языки**

  Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.

### См. также:

Синхронизация обновлений Windows Update с Сервером администрирования ..... 494

Сценарий:Обновление программ сторонних производителей ..... 489

## Шаг 5. Выбор учетной записи для запуска задачи

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию**

  Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

  По умолчанию выбран этот вариант.

- **Задать учетную запись**

  В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

## См. также:

Синхронизация обновлений Windows Update с Сервером администрирования ..... 494

Сценарий:Обновление программ сторонних производителей ..... 489

## Шаг 6. Настройка расписания запуска задачи

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Один раз**
- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо

сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

### См. также:

Синхронизация обновлений Windows Update с Сервером администрирования ..... 494

Сценарий:Обновление программ сторонних производителей ..... 489

## Шаг 7. Определение названия задачи

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).По умолчанию задано значение *Синхронизация обновлений Windows Update*.

### См. также:

Синхронизация обновлений Windows Update с Сервером администрирования ..... 494

Сценарий:Обновление программ сторонних производителей ..... 489

### Шаг 8. Завершение создания задачи

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

Созданная задача синхронизации обновлений Windows Update отобразится в списке задач в папке **Задачи** дерева консоли.

### См. также:

Синхронизация обновлений Windows Update с Сервером администрирования .....494

Сценарий:Обновление программ сторонних производителей .....489

## Установка обновлений на устройства вручную

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Остановить или запустить задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

Если в мастере первоначальной настройки вы выбрали вариант **Искать требующиеся для установки обновления**, вы можете установить обновления программного обеспечения на клиентские устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки обновлений.
- Добавьте правило для установки обновления в существующую задачу установки обновлений.
- В параметрах существующей задачи установки обновлений настройте тестовую установку обновлений.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

#### Установка обновлений с помощью создания задачи установки обновлений

Вы можете выполнить одно из следующих действий:

- Создайте задачу для установки требуемых обновлений.
- Выберите обновление и создайте задачу для его установки и для установки аналогичных обновлений.

► *Чтобы установить требуемые обновления:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области папки выберите обновление, которое вы хотите установить.

3. Выполните одно из следующих действий:

   - В контекстном меню выбранного обновления выберите пункт **Установить обновление** → **Создать задачу**.
   - Перейдите по ссылке **Установить обновление (создать задачу)** в блоке работы с выбранным обновлением.

4. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

5. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

     - **Повторять запрос каждые (мин)**

       Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

       По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

       Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагружать через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Вы можете включить автоматическую установку общесистемных компонентов (пререквизитов), перед установкой обновления в свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей*. Когда параметр включен, все требуемые общесистемные компоненты устанавливаются перед обновлением. Список этих компонентов можно посмотреть в свойствах обновления.

В свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей* вы можете разрешить установку обновлений, которые обновляют программу до новой версии.

Если в параметрах задачи настроены правила установки обновлений сторонних производителей, Сервер администрирования загружает с сайта производителей требуемые обновления. Обновления сохраняются в хранилище Сервера администрирования и далее распространяются и устанавливаются на устройства, где они применимы.

Если в параметрах задачи настроены правила установки обновлений Microsoft и Сервер администрирования используется в качестве WSUS-сервера, Сервер администрирования загружает необходимые обновления в хранилище и далее распространяет на управляемые устройства. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

► *Чтобы установить требуемое обновление и аналогичные обновления:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   > Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.
4. В окне **Поиск существующих задач установки обновления** задайте следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

- **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Создать задачу установки обновления**.
2. Выберите тип правила установки, чтобы добавить его в новую задачу и нажмите на кнопку **Готово**.

3. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.

4. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

     - **Повторять запрос каждые (мин)**

       Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

       По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

       Если параметр выключен, предложение перезагрузки отображается только один раз.

     - **Принудительно перезагружать через (мин)**

       После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

       По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих параметров:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

   - **Назначить задачу группе администрирования**

     В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную** (выбрано по умолчанию)

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

После завершения работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

После установки новой версии программы может быть нарушена работа других программ, установленных на устройствах и зависящих от работы обновляемой программы.

**Установка обновления с помощью добавления правила в существующую задачу**

► *Чтобы установить обновление с помощью добавления правила в существующую задачу:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Обновления программного обеспечения**.
2. В рабочей области выберите обновление, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления.

   Функционал мастера установки обновления доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.

4. В окне **Поиск существующих задач установки обновления** задайте следующие параметры:

   - **Искать задачи, устанавливающие выбранное обновление**

Если этот параметр включен, мастер установки обновления ищет существующую задачу, чтобы установить выбранное обновление.

Если этот параметр выключен или если не было найдено подходящей задачи, мастер установки обновления предлагает создать правило или задачу для установки обновления.

По умолчанию параметр включен.

   - **Одобрить установку обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

1. Если вы выбрали поиск существующей задачи для установки обновлений и было найдено несколько подходящих задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае, нажмите на кнопку **Добавить правило установки обновления**.

2. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

3. Выберите тип правила, которое будет добавлено в выбранную задачу, и нажмите на кнопку **Готово**.

4. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

Новое правило для установки обновления добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

**Настройка проверочной установки обновлений**

► *Чтобы настроить проверочную установку обновлений:*

1. В дереве консоли в папке **Управляемые устройства** на закладке **Задачи** выберите задачу **Установка требуемых обновлений и закрытие уязвимостей**.

2. В контекстном меню задачи выберите пункт **Свойства**.

   Откроется окно свойств задачи **Установка требуемых обновлений и закрытие уязвимостей**.

3. В окне свойств задачи в разделе **Проверочная установка** выберите один из доступных вариантов проверочной установки:

   - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.

   - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

- **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
- **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

4. После выбора любого параметра, кроме **Не проверять**, в поле **Время для принятия решения о продолжении установки (ч.)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

См. также:

Сценарий:Обновление программ сторонних производителей .....489

## Настройка обновлений Windows в политике Агента администрирования

► *Чтобы настроить обновления Windows в политике Агента администрирования:*

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области выберите закладку **Политики**.
3. Выберите политику Агента администрирования.
4. В контекстном меню политики выберите пункт **Свойства**.

   Откроется окно свойств политики Агента администрирования.
5. В окне свойств политики Агента администрирования выберите раздел **Обновления и уязвимости в программах**.
6. Включите параметр **Использовать Сервер администрирования в роли WSUS-сервера**, чтобы загружать обновления Windows на Сервер администрирования и затем распространять их на клиентские устройства средствами Агента администрирования.

   Если этот параметр не выбран, обновления Windows загружаются на Сервер администрирования. В этом случае клиентские устройства получают обновления Windows напрямую с серверов Microsoft.
7. Выберите набор обновлений, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

   Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

   Выберите параметр из раскрывающегося списка:

   - **Устанавливать все применимые обновления Центра обновления Windows**

     Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

     Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

1. Выберите режим поиска обновлений Windows Update:

- **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от Агента Центра обновления Windows.

Этот параметр вступает в силу только в том случае, если параметр **Соединяться с сервером обновлений для актуализации данных** задачи *Поиск уязвимостей и требуемых обновлений* включен.

По умолчанию выбран этот вариант.

- **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

Выберите этот параметр, если вы хотите получать обновления из кеша источника обновлений.

- **Выключен**

  Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

  Выберите этот параметр, если, например, вы хотите сначала протестировать обновления на локальном устройстве.

2. Включите параметр **Проверять исполняемые файлы на наличие уязвимостей при запуске**, чтобы при запуске исполняемых файлов выполнять их проверку на наличие уязвимостей.
3. Убедитесь, что редактирование заблокировано для всех параметров, которые вы изменили. В противном случае изменения не применяются.
4. Нажмите на кнопку **Применить**.

См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

## Уязвимости в программах

Папка **Уязвимости в программах**, входящая в состав папки **Управление программами**, содержит список уязвимостей в программах, которые обнаружил на клиентских устройствах установленный на них Агент администрирования. Агент администрирования выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях.

Функциональность анализа информации об уязвимостях в программах поддерживается только для операционных систем Microsoft Windows.

Открыв окно свойств выбранной программы в папке **Уязвимости в программах**, вы можете получить общую информацию об уязвимости, о программе, в которой она обнаружена, просмотреть список устройств, на которых обнаружена уязвимость, а также информацию о закрытии уязвимости.

Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (https://threats.kaspersky.com/ru/).

kaspersky

## В этом разделе



# Сценарий: Обнаружение и закрытие уязвимостей в программах сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционных системах, в программах сторонних производителей, включая программы Microsoft (см. стр. 1275).

### Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в программах Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в программах сторонних производителей, отличных от программ Microsoft.

### Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

**a. Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах**

Чтобы найти уязвимости в программах, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в программах (см. стр. 522), Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (см. стр. 1289), параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

**b. Анализ списка обнаруженных уязвимостей в программах**

Просмотрите список **Уязвимости в программах** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации об уязвимостях в программах (см. стр. 520), Просмотр статистики уязвимостей на управляемых устройствах (см. стр. 521).
- Kaspersky Security Center 14.2 Web Console: Просмотр информации об уязвимостях в программах (см. стр. 1331), Просмотр статистики уязвимостей на управляемых устройствах (см. стр. 1333).

**c. Настройка закрытия уязвимостей**

Обнаружив уязвимости в программах, вы можете закрыть уязвимости в программах на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295) или задачу *Закрытие уязвимостей* (см. стр. 1320).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в программах сторонних производителей, включая программы Microsoft, установленные на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Для закрытия уязвимостей в программах в задаче *Установка требуемых обновлений и закрытия уязвимостей* используются рекомендуемые обновления программного обеспечения.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в программах сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления программ Microsoft и пользовательские исправления для программ сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в программах сторонних производителей (см. стр. 549), Закрытие уязвимостей в программах (см. стр. 527).
- Kaspersky Security Center 14.2 Web Console: Пользовательские исправления для уязвимостей в программах сторонних производителей (см. стр. 1330), Закрытие уязвимостей в программах сторонних производителей (см. стр. 1316), Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295).

**d. Задание расписания задачи**

Чтобы убедится, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей* вы должны выбрать исправления программ Microsoft или указать пользовательские исправления для программ сторонних производителей каждый раз перед запуском задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

**e. Игнорирование уязвимостей в программах (если требуется)**

Вы можете игнорировать уязвимости в программах, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

Инструкции:

- Консоль администрирования: Игнорирование уязвимостей в программах (если требуется) (см. стр. 548).
- Kaspersky Security Center 14.2 Web Console: Игнорирование уязвимостей в программах (если требуется) (см. стр. 1334).

**f. Запуск задачи закрытия уязвимости**

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

**g. Создание отчета о результатах закрытия уязвимостей в программах (если требуется)**

Чтобы просмотреть статистику о закрытии уязвимостей, сформируйте отчет об уязвимостях. В отчете отображается информация об уязвимостях в программах, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в программах сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (см. стр. 588).
- Kaspersky Security Center 14.2 Web Console: Генерация и просмотр отчета (см. стр. 1372).

**h. Проверка настройки обнаружения и закрытия уязвимостей в программах сторонних производителей**

Убедитесь, что вы выполнили следующее:

- обнаружили и просмотрели список уязвимостей в программах на управляемых устройствах;
- игнорировали уязвимости в программах, если хотели;
- настроили задачу закрытия уязвимости;
- запланировали запуск задач для поиска и закрытия уязвимостей в программах так, чтобы они запускались последовательно;
- проверили, что задача закрытия уязвимостей была запущена.

**Результаты**

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в программах.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в программах Microsoft.

См. также:

О программах сторонних производителей ..... 1275

## Об обнаружении и закрытии уязвимостей в программах

Kaspersky Security Center обнаруживает и закрывает уязвимости в программах на управляемых устройствах под управлением операционных систем семейства Microsoft Windows. Уязвимости обнаруживаются в операционных системах и в программах сторонних производителей, включая программное обеспечение Microsoft (см. стр. 1275).

### Обнаружение уязвимостей в программах

Для обнаружения уязвимостей Kaspersky Security Center выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях. Эта база формируются специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (https://threats.kaspersky.com/ru/).

Kaspersky Security Center использует задачу *Поиск уязвимостей и требуемых обновлений* для поиска уязвимостей в программах.

### Закрытие уязвимостей в программах

Для закрытия уязвимостей в программах, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для программ "Лаборатории Касперского" и программ сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования (см. стр. 1244) может быть создана вручную.
- *Синхронизация обновлений Windows Update*. Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости программного обеспечения, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимости в программах используйте задачу *Установка требуемых обновлений и закрытия уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для программ Microsoft и пользовательских исправлений для программ сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений программ сторонних производителей, которые можно установить с помощью Системного администрирования. Кроме того, специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях, и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вы должны принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

## См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Просмотр информации об уязвимостях в программах

► *Чтобы просмотреть список уязвимостей, обнаруженных на клиентских устройствах,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.

Отобразится страница со списком уязвимостей в программах, обнаруженных на управляемых устройствах.

► *Чтобы получить информацию о выбранной уязвимости,*

В контекстном меню уязвимости выберите пункт **Свойства**.

Откроется окно свойств уязвимости, в котором отображается следующая информация:

- программа, в которой обнаружена уязвимость;
- список устройств, на которых обнаружена уязвимость;
- информация о закрытии уязвимости.

► *Чтобы просмотреть отчет обо всех обнаруженных уязвимостях,*

В папке **Уязвимости в программах** воспользуйтесь ссылкой **Просмотреть отчет об уязвимостях в программах**.

Будет создан отчет об уязвимостях в программах, установленных на устройствах. Отчет можно просмотреть в узле с именем нужного вам Сервера администрирования на закладке **Отчеты**.

## См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей.....516

## Просмотр статистики уязвимостей на управляемых устройствах

Вы можете просмотреть статистическую информацию каждой уязвимости в программах на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на: <количество устройств>*. Статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на: <количество устройств>*. Статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на: <количество устройств>*. Статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на: <количество устройств>*. Статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требует закрытия на: <количество устройств>*. Статус присваивается, если уязвимость была закрыта только на части управляемых устройств, и ее необходимо закрыть на остальных управляемых устройствах.

► *Чтобы просмотреть статистику уязвимости на управляемых устройствах:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.

   Отобразится страница со списком уязвимостей в программах, обнаруженных на управляемых устройствах.

2. Выберите уязвимость для которой вы хотите просмотреть статистику.

   В блоке для работы с выбранным объектом отображается диаграмма состояний уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Поиск уязвимостей в программах

Если вы выполнили настройку программы с помощью мастера первоначальной настройки, задача *Поиск уязвимостей* создается автоматически. Просмотреть задачу можно в папке **Управляемые устройства** на закладке **Задачи**.

► *Чтобы создать задачу поиска уязвимостей в программах, установленных на клиентских устройствах:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами**, выберите вложенную папку **Уязвимости в программах**.
2. В рабочей области папки нажмите на кнопку **Дополнительные действия** → **Настроить поиск уязвимостей**.

   Если задача для поиска уязвимостей уже существует, она отображается на закладке **Задачи** в папке **Управляемые устройства**, с существующими выбранными задачами. В противном случае запускается мастер создания задачи поиска уязвимостей и требуемых обновлений. Следуйте далее указаниям мастера.
3. В окне **Выбор типа задачи** выберите **Поиск уязвимостей и требуемых обновлений**.
4. В окне мастера **Параметры**, укажите следующие параметры задачи:
   - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних программ.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на клиентском устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. 750)).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы

можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в программах**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления только если параметр **Соединяться с сервером обновлений для актуализации данных** включен и параметр **Активный** включен в группе параметров **Режим поиска обновлений Windows Update**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска обновлений Windows Update** или если параметр **Соединяться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Активный**.
- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Выключен**, Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в

утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

    - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с

указанного времени, в день создания задачи.

По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности,

сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача Поиск уязвимостей и требуемых обновлений, которая отображается в списке задач, в папке **Управляемые устройства**, на закладке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Когда задача *Поиск уязвимостей и требуемых обновлений* завершена, Сервер администрирования отображает список уязвимостей, обнаруженных в программах, установленных на устройстве; также Сервер отображает все обновления программного обеспечения, необходимые для исправления обнаруженных уязвимостей.

Если результаты задачи содержат ошибку 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

Сервер администрирования не отображает список необходимых обновлений программного обеспечения при последовательном запуске двух задач: задачи *Синхронизация обновлений Windows Update*, для которой отключен параметр **Загружать файлы экспресс-установки**, и затем задачи *Поиск уязвимостей и требуемых обновлений*. Чтобы просмотреть список необходимых обновлений программного обеспечения, необходимо снова запустить задачу *Поиск уязвимостей и требуемых обновлений*.

Агент администрирования получает информацию о любых доступных обновлениях Windows и других программ Microsoft от Центра обновления Windows или от Сервера администрирования, если Сервер администрирования выполняет роль WSUS-сервера. Информация передается при запуске программ (если это предусмотрено политикой) и при каждом запуске задачи *Поиск уязвимостей и требуемых обновлений* на клиентских устройствах.

Вы можете получить сведения о программном обеспечении сторонних производителей, которое можно обновлять с помощью Kaspersky Security Center на веб-сайте Службы технической поддержки на странице Kaspersky Security Center, в разделе **Управление Сервером** (**https://support.kaspersky.ru/14758**).

## См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

Сценарий:Обновление программ сторонних производителей .....489

## Закрытие уязвимостей в программах

Если в мастере первоначальной настройки в окне **Параметры управления обновлениями** вы выбрали вариант **Искать и устанавливать требующиеся обновления**, задача *Установка требуемых обновлений и закрытие уязвимостей* создается автоматически. Задача отображается в папке **Управляемые устройства** на закладке **Задачи**.

В противном случае вы можете выполнить одно из следующих действий:

- Создайте задачу для закрытия уязвимостей с помощью установки доступных обновлений.
- Добавьте правило для закрытия уязвимостей в существующую задачу закрытия уязвимостей.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

**Закрытие уязвимостей с помощью задачи закрытия уязвимостей**

Вы можете выполнить одно из следующих действий:

- Создайте задачу закрытия нескольких уязвимостей, соответствующих определенным правилам.
- Выберите уязвимость и создайте задачу для ее закрытия и для закрытия аналогичных уязвимостей.

► *Чтобы закрыть уязвимости, которые соответствуют определенным правилам:*

1. В дереве консоли выберите Сервер администрирования, на устройствах которого вы хотите закрыть уязвимости.
2. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
3. В открывшемся окне установите флажок **Отображать Системное администрирование** и нажмите на кнопку **ОК**.
4. В окне с сообщением программы нажмите на кнопку **ОК**.
5. Перезапустите Консоль администрирования, чтобы изменения вступили в силу.
6. В дереве консоли откройте папку **Управляемые устройства**.
7. В рабочей области выберите закладку **Задачи**.
8. По кнопке **Создать задачу** запустите мастер создания задачи. Следуйте далее указаниям мастера.
9. В окне **Выбор типа задачи** мастера создания задачи выберите **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. стр. 771) **Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
10. В окне мастера **Параметры**, укажите следующие параметры задачи:

    - **Задайте правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений (см. стр. 550).

- **Начинать установку в момент перезагрузки или выключения устройства**

  Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

  Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

  Если этот параметр выключен, необходимо установить пререквизиты вручную.

  По умолчанию параметр выключен.

- **Разрешать установку новой версии программы при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

  Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине

значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагружать через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

Если результаты задачи содержат ошибку 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

► *Чтобы закрыть требуемую уязвимость и аналогичные ей:*

1. В дереве консоли в папке **Дополнительно → Управление программами** выберите вложенную папку **Уязвимости в программах**.
2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

   Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.
4. В окне **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:
   - **Искать задачи, закрывающие выбранную уязвимость**

     Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

     Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

     По умолчанию параметр включен.
   - **Одобрить обновления, закрывающие выбранную уязвимость**

     Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

     По умолчанию параметр выключен.
5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Новая задача закрытия уязвимости**.

6. Выберите тип правила, закрывающего уязвимость, чтобы добавить его в существующую задачу и нажмите на кнопку **Готово**.
7. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

   Откроется мастер создания задачи установки обновлений и закрытия уязвимостей. Следуйте далее указаниям мастера.
8. В окне мастера **Выбор варианта перезагрузки операционной системы** выберите действие, которое необходимо выполнить, если операционная система на клиентских устройствах должна быть перезапущена после операции:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

     - **Повторять запрос каждые (мин)**

       Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

       По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

       Если параметр выключен, предложение перезагрузки отображается только один раз.

     - **Принудительно перезагружать через (мин)**

       После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

       По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. В окне мастера **Выбор устройств, которым будет назначена задача** выберите один из следующих параметров:

   - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

     В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

     Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

   - **Назначить задачу группе администрирования**

     В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

2. В окне мастера **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости настройте следующие параметры:

   - **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

   - **Каждый N час**

Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда

в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
2. В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

В результате работы мастера создается задача **Установка требуемых обновлений и закрытие уязвимостей**, которая отображается в папке **Задачи**.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

**Закрытие уязвимости с помощью добавления правила в существующую задачу закрытия уязвимостей**

► *Чтобы закрыть уязвимость с помощью добавления правила в существующую задачу закрытия уязвимостей:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.
2. Выберите уязвимость, которую вы хотите закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости.

   Функционал мастера закрытия уязвимости доступен при наличии лицензии на Системное администрирование.

   Следуйте далее указаниям мастера.
4. В окне **Поиск существующих задач закрытия уязвимости** укажите следующие параметры:

   - **Искать задачи, закрывающие выбранную уязвимость**

     Если этот параметр включен, мастер закрытия уязвимости выполняет поиск существующих задач для закрытия выбранной уязвимости.

Если этот параметр выключен или не было найдено применимых задач, мастер закрытия уязвимости предлагает создать правило или задачу для закрытия уязвимости.

По умолчанию параметр включен.

- **Одобрить обновления, закрывающие выбранную уязвимость**

  Обновления, которые закрывают уязвимость, будут одобрены к установке. Включите этот параметр, если некоторые применяемые правила установки обновлений разрешают установку только одобренных обновлений.

  По умолчанию параметр выключен.

5. Если для закрытия уязвимости вы выбрали поиск существующих задач и было найдено несколько задач, вы можете просмотреть свойства этих задач или запустить их вручную. Никаких дальнейших действий не требуется.

   В противном случае нажмите на кнопку **Добавить правило закрытия уязвимости в существующую задачу**.

6. Выберите задачу, для которой вы хотите добавить правило и нажмите на кнопку **Добавить правило**.

   Также вы можете просмотреть свойства существующих задач, запустить их вручную или создать задачу.

7. Выберите тип правила, чтобы добавить его в выбранную задачу, и нажмите на кнопку **Готово**.

8. Откроется окно установки всех предыдущих версий программы. Нажмите **Да**, если вы согласны на последовательную установку версий программы, если это необходимо для установки выбранных обновлений. Нажмите **Нет**, если вы хотите непосредственно обновить программу, не устанавливая последовательно версии. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

Новое правило для закрытия уязвимости добавлено в существующую задачу **Установка требуемых обновлений и закрытие уязвимостей**.

### См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

## Закрытие уязвимостей в изолированной сети

В этом разделе описаны действия, которые вы можете предпринять для закрытия уязвимостей в программах сторонних производителей на управляемых устройствах, подключенных к Серверам администрирования и не имеющих доступа в интернет.

kaspersky

## В этом разделе



## Сценарий: Закрытие уязвимостей программ сторонних производителей в изолированной сети

Вы можете устанавливать обновления и закрывать уязвимости программ сторонних производителей, установленных на управляемых устройствах в изолированной сети. К таким сетям относятся Серверы администрирования и подключенные к ним управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходим Сервер администрирования, подключенный к интернету. Также вы можете загружать патчи (требуемые обновления) с помощью Сервера администрирования с доступом в интернет и передавать исправления на изолированные Серверы администрирования.

Вы можете загружать обновления программ сторонних производителей, выпущенные производителями программного обеспечения, но не можете загружать обновления для программного обеспечения Microsoft на изолированных Серверах администрирования с помощью Kaspersky Security Center.

Чтобы узнать, как работает процесс закрытия уязвимостей в изолированной сети, ознакомьтесь с описанием и схемой этого процесса (см. стр. 542).

**Предварительные требования**

Прежде чем начать, сделайте следующее:

1. Выделите одно устройство для подключения к интернету и загрузки исправлений. Это устройство будет считаться Сервером администрирования с доступом в интернет.
2. Установите Kaspersky Security Center (см. стр. 92) версии не ниже 14 на следующих устройствах:
   - Выделенное устройство, которое будет выступать в роли Сервера администрирования с доступом в интернет.
   - Изолированные устройства, которые будут выступать в роли изолированных от интернета Серверов администрирования (далее – изолированные Серверы администрирования).
3. Убедитесь, что на каждом Сервере администрирования достаточно места на диске для загрузки и хранения обновлений и исправлений.

**Этапы**

Установка обновлений и закрытие уязвимостей программ сторонних производителей на управляемых устройствах, относящихся к изолированным Серверам администрирования, состоит из следующих этапов:

a. **Настройка Сервера администрирования с доступом в интернет**

Подготовьте Сервер администрирования с доступом в интернет (см. стр. 543) для обработки запросов на необходимые обновления стороннего программного обеспечения и для загрузки.

b. **Настройка изолированных Серверов администрирования**

Подготовьте изолированные Серверы администрирования (см. стр. 544), чтобы они могли регулярно формировать списки необходимых обновлений и обрабатывать патчи, загружаемые Сервером администрирования с доступом в интернет. После настройки изолированные Серверы администрирования больше не пытаются загружать патчи из интернета. Вместо этого они получают обновления через патчи.

c. **Передача патчей и установка обновлений на изолированные Серверы администрирования**

После завершения настройки Серверов администрирования вы можете передавать необходимые списки обновлений и патчей (см. стр. 545) между Сервером администрирования с доступом в интернет и изолированными Серверами администрирования. Далее обновления из патчей будут установлены на управляемые устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

**Результаты**

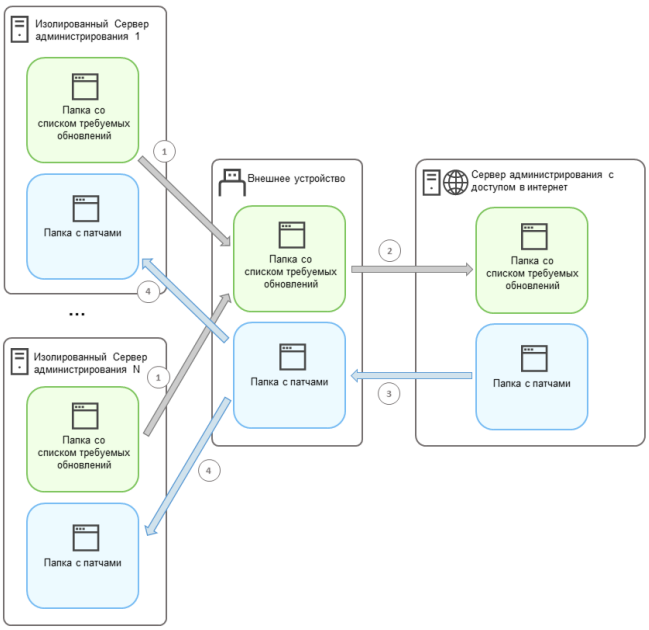
Таким образом обновления программ сторонних производителей передаются на изолированные Серверы администрирования и устанавливаются на подключенные управляемые устройства с помощью Kaspersky Security Center. Достаточно один раз настроить Серверы администрирования, чтобы получать обновления с нужной вам частотой, например, один или несколько раз в день.

## См. также:

Выключение возможности передачи исправлений и установки обновлений в изолированной сети547

## О закрытии уязвимостей программ сторонних производителей в изолированной сети

Процесс закрытия уязвимостей в программах сторонних производителей в изолированной сети (см. стр. 541) показан на рисунке и описан ниже. Вы можете периодически повторять этот процесс.



Каждый Сервер администрирования, изолированный от сети интернет (далее — изолированный Сервер администрирования), формирует список обновлений, которые необходимо установить на управляемые устройства, подключенные к данному Серверу администрирования. Список необходимых обновлений хранится в специальной папке и представляет собой набор бинарных файлов. Каждый файл имеет имя, которое содержит идентификатор патча с требуемым обновлением. В результате каждый файл в списке указывает на определенный патч.

С помощью внешнего устройства вы переносите список необходимых обновлений с изолированного Сервера администрирования на выделенный Сервер администрирования с доступом в интернет. После этого выделенный Сервер администрирования загружает патчи из интернета и помещает их в отдельную папку.

Когда все патчи загружены и размещены в специальной для них папке, вы перемещаете патчи на каждый изолированный Сервер администрирования, с которого вы взяли список необходимых обновлений. Вы сохраняете патчи в специально созданную для них папку на изолированном Сервере администрирования. В результате задача *Установка требуемых обновлений и закрытия уязвимостей* запускает патчи и устанавливает обновления на управляемые устройства изолированных Серверов администрирования.

## См. также:

Сценарий:Закрытие уязвимостей программ сторонних производителей в изолированной сети .....541

Передача исправлений и установка обновлений в изолированной сети .....545

## Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети

Чтобы подготовиться к закрытию уязвимостей и передаче патчей (см. стр. 541) в изолированной сети, сначала настройте Сервер администрирования с доступом в интернет, а затем настройте изолированные Серверы администрирования (см. стр. 544).

► *Чтобы настроить Сервер администрирования с доступом в интернет:*

1. Создайте две папки (см. стр. 542) на диске, где установлен Сервер администрирования:
   - папку для списка необходимых обновлений;
   - папку для патчей.

   Название папок может быть любым.
2. Предоставьте группе KLAdmins (см. стр. 675) право Изменение на созданные папки, используя стандартные средства администрирования операционной системы.
3. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования. Введите следующие команды в командной строке Windows с правами администратора:
   - Чтобы указать путь к папке для исправлений:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"
   ```

   - Чтобы задать путь к папке для списка необходимых обновлений:

   ```
   klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"
   ```

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches"`

4. С помощью утилиты klscflag укажите, как часто Сервер администрирования должен проверять наличие новых запросов на исправления (если требуется):

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <value in seconds>
```

По умолчанию указано значение 120 секунд.

Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

5. Перезапустите службу Сервера администрирования.

Теперь Сервер администрирования с доступом в интернет готов к загрузке и передаче обновлений на изолированные Серверы администрирования. Прежде чем приступить к закрытию уязвимостей, настройте изолированные Серверы администрирования (см. стр. 544).

## См. также:



## Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

После того, как настройка Сервера администрирования с доступом в интернет (см. стр. 543) закончена, подготовьте каждый изолированный Сервер администрирования в вашей сети, чтобы вы могли закрывать уязвимости и устанавливать обновления (см. стр. 541) на управляемых устройствах, подключенных к изолированным Серверам администрирования.

► *Чтобы настроить изолированные Серверы администрирования на каждом из них:*

1. Активируйте лицензионный ключ (см. стр. 357) для Системного администрирования.
2. Создайте две папки (см. стр. 542) на диске, где установлен Сервер администрирования:
   - папку, в которой появится список необходимых обновлений;
   - папку для патчей.

   Название папок может быть любым.
3. Предоставьте группе KLAdmins (см. стр. 675) право *Изменение* на созданные папки, используя стандартные средства администрирования операционной системы.
4. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования. Введите следующие команды в командной строке Windows с правами администратора:
   - Чтобы указать путь к папке для исправлений:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<путь к папке>"
   ```

   - Чтобы задать путь к папке для списка необходимых обновлений:

   ```
   klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"
   ```

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches"`

5. С помощью утилиты klscflag укажите, как часто изолированный Сервер администрирования должен проверять наличие новых патчей (если требуется):

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>
   ```

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

6. Используйте утилиту klscflag для вычисления хешей SHA-256 патчей (если требуется):

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```

   Введя эту команду, вы можете убедиться, что патчи не были изменены при их переносе на изолированный Сервер администрирования и что вы получили корректные патчи, содержащие необходимые обновления.

   По умолчанию Kaspersky Security Center не вычисляет хеши SHA-256 патчей. Если включить этот параметр, после получения патчей изолированным Сервером администрирования Kaspersky Security Center вычисляет их хеши и сравнивает полученные значения с хешами, хранящимися в базе данных Сервера администрирования. Если вычисленный хеш не совпадает с хешем в базе данных, возникает ошибка и вам необходимо заменить неверные патчи.

7. Создайте задачу (см. стр. 1289) *Поиск уязвимостей и требуемых обновлений* и установите расписание задачи (см. стр. 1292). Запустите задачу, если вы хотите, чтобы она выполнялась раньше, чем указано в расписании задачи.

8. Перезапустите службу Сервера администрирования.

После настройки всех Серверов администрирования вы можете переместить исправления и списки необходимых обновлений (см. стр. 545) и закрыть уязвимости программ сторонних производителей на управляемых устройствах в изолированной сети.

## См. также:

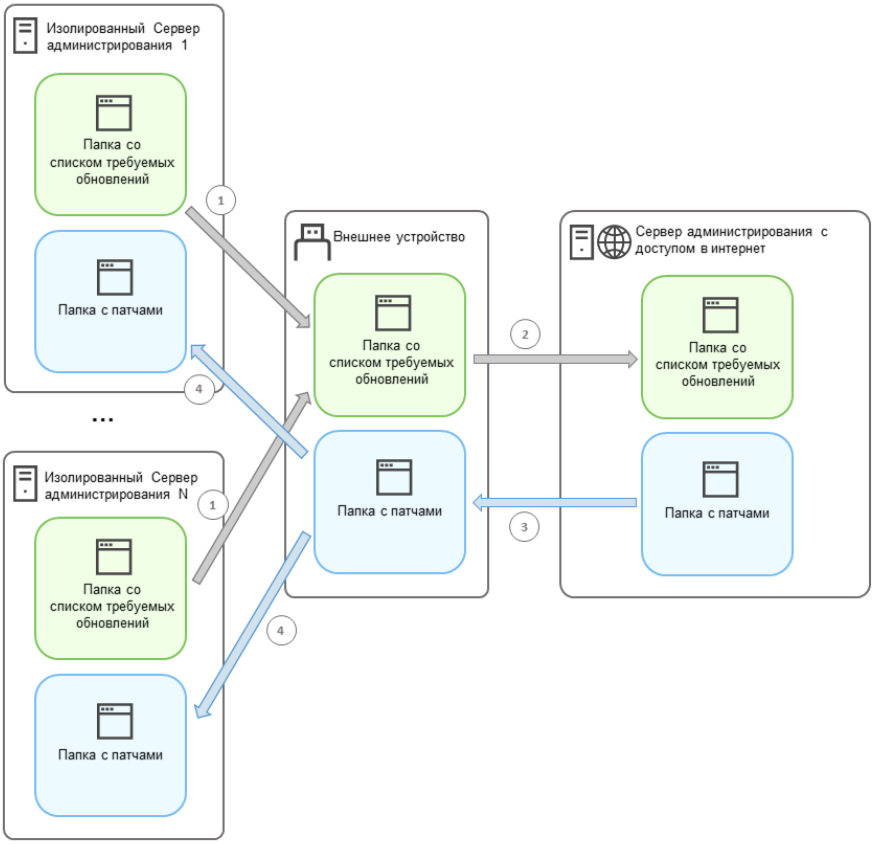


## Передача исправлений и установка обновлений в изолированной сети

После того, как настройка Серверов администрирования (см. стр. 541) закончена, вы можете переносить патчи с необходимыми обновлениями с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Вы можете передавать и устанавливать обновления с нужной вам частотой, например, один или несколько раз в день.

Съемный диск, например, внешний диск, необходим, для переноса патчей и списка необходимых обновлений между Серверами администрирования. Убедитесь, что внешний диск имеет достаточно места для загрузки и хранения патчей.

Процесс передачи патчей и списка необходимых обновлений показан на рисунке и описан ниже:




► *Чтобы установить обновления и закрыть уязвимости на управляемых устройствах, подключенных к изолированным Серверам администрирования:*

1. Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*, если она еще не запущена.
2. Подключите внешний диск к любому изолированному Серверу администрирования.
3. Создайте на внешнем диске две папки: одну для списка необходимых обновлений и одну для патчей. Название папок может быть любым.

   Если вы создали эти папки ранее, очистите их.
4. Скопируйте список необходимых обновлений с каждого изолированного Сервера администрирования и вставьте этот список в папку для списка необходимых обновлений на внешнем диске.

   В результате вы объединяете все списки, полученные со всех изолированных Серверов администрирования, в одну папку. В этой папке должны находиться бинарные файлы (см. стр. 542) с идентификаторами патчей, необходимых для всех изолированных Серверов администрирования.
5. Подключите внешний диск к Серверу администрирования с доступом в интернет.
6. Скопируйте список необходимых обновлений с внешнего диска и вставьте этот список в папку для списка необходимых обновлений на Сервере администрирования с доступом в интернет.

   Все необходимые патчи автоматически загружаются из интернета в папку патчей на Сервере администрирования. Это может занять несколько часов.

7. Убедитесь, что все необходимые патчей загружены. Для этого можно выполнить одно из следующих действий:

   - Проверьте папку на наличие патчей на Сервере администрирования с доступом в интернет. Все исправления, которые были указаны в списке необходимых обновлений, должны быть загружены в нужную папку. Это удобнее, если требуется небольшое количество исправлений.
   - Подготовьте специальный скрипт, например, shell-скрипт. Если вы получите большое количество патчи, то будет сложно самостоятельно проверить, что все исправления загружены. В таких случаях лучше автоматизировать проверку.

8. Скопируйте патчи с Сервера администрирования с доступом в интернет и вставьте их в соответствующую папку на внешнем диске.
9. Перенесите исправления на каждый изолированный Сервер администрирования. Поместите патчи в специальную папку для них.

В результате каждый изолированный Сервер администрирования формирует актуальный список обновлений, необходимых для управляемых устройств, подключенных к текущему Серверу администрирования. После получения списка необходимых обновлений Сервер администрирования загружает из интернета патчи. При появлении этих патчей на изолированных Серверах администрирования задача *Установка требуемых обновлений и закрытие уязвимостей* обрабатывает эти патчи. Таким образом, на управляемые устройства устанавливаются обновления и закрываются уязвимости в программах сторонних производителей.

Когда задача *Установка требуемых обновлений и закрытие уязвимостей* запущена, не перезагружайте устройство Сервера администрирования и не запускайте задачу *Резервное копирование данных Сервера администрирования* (это также вызовет перезагрузку). В результате задача *Установка требуемых обновлений и закрытие уязвимостей* прерывается, а обновления не устанавливаются. В этом случае вам необходимо перезапустить эту задачу вручную или дождаться запуска задачи по настроенному расписанию.

## См. также:

Сценарий:Закрытие уязвимостей программ сторонних производителей в изолированной сети .....541

О закрытии уязвимостей программ сторонних производителей в изолированной сети.....542

## Выключение возможности передачи исправлений и установки обновлений в изолированной сети

Вы можете выключить передачу исправлений (см. стр. 545) на изолированные Сервера администрирования, например, если вы решили вывести один или несколько Серверов администрирования из изолированной сети. Таким образом вы сможете уменьшить количество исправлений и время на их загрузку.

► *Чтобы отключить возможность передачи патчей на изолированные Серверы администрирования:*

1. Если вы хотите вывести из изоляции все Серверы администрирования, в свойствах Сервера администрирования с доступом в интернет удалите пути к папкам для патчей и список необходимых обновлений. Если вы хотите, чтобы некоторые Серверы администрирования находились в изолированной сети, пропустите этот шаг.

   Введите следующие команды в командной строке Windows с правами администратора:

- Чтобы удалить путь к папке с исправлениями:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
```

- Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
```

2. Перезапустите службу Сервера администрирования, если вы удалили пути к папкам на этом Сервере администрирования.
3. В свойствах каждого Сервера администрирования, который вы хотите вывести из изоляции, удалите пути к папкам для патчей и список необходимых обновлений.

   Введите следующие команды в командной строке Windows с правами администратора:

   - Чтобы удалить путь к папке с исправлениями:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
```

   - Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
```

4. Перезапустите службу каждого Сервера администрирования, на котором вы удалили пути к папкам.

Если вы перенастроили Сервер администрирования с доступом в интернет, вы больше не будете получать патчи через Kaspersky Security Center. Если вы перенастроили только некоторые изолированные Серверы администрирования, например, вынеся некоторые из них из изолированной сети, вы получите патчи только для остальных изолированных Серверов администрирования.

Если вы хотите в будущем приступить к закрытию уязвимостей на отключенных изолированных Серверах администрирования, вам необходимо настроить эти Серверы администрирования и Сервер администрирования с доступом в интернет (см. стр. 541) еще раз.

### См. также:

Сценарий:Закрытие уязвимостей программ сторонних производителей в изолированной сети .....541

О закрытии уязвимостей программ сторонних производителей в изолированной сети.....542

## Игнорирование уязвимостей в программах

Вы можете игнорировать уязвимости в программах и не закрывать их. Причины для игнорирования уязвимостей в программах могут быть, например, следующими:

- Вы не считаете уязвимость в программе критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в программах может повредить данные программы, для которой требуется закрыть уязвимость.
- Вы уверены, что уязвимость в программах не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в программах на всех управляемых устройствах или только на выбранных управляемых устройствах.

► *Чтобы пропустить уязвимость в программах на всех управляемых устройствах:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.

В рабочей области папки отображается список уязвимостей в программах на устройствах, которые обнаружил Агент администрирования, установленный на них.

2. Выберите уязвимость, которую вы хотите пропустить.
3. В контекстном меню уязвимости выберите пункт **Свойства**.

   Откроется окно свойств уязвимости.
4. В разделе **Общие** установите флажок **Игнорировать уязвимость**.
5. Нажмите на кнопку **ОК**.

   Окно свойств уязвимости в программах закроется.

Уязвимость в программах пропускается на всех управляемых устройствах.

► *Чтобы пропустить уязвимость в программах на выбранных управляемых устройствах:*

1. Откройте окно свойств выбранного управляемого устройства (см. стр. 742) и выберите раздел **Уязвимости в программах**.
2. Выберите уязвимость в программах.
3. Пропустите выбранную уязвимость.

Уязвимость в программах пропускается на выбранном устройстве.

Пропущенная уязвимость в программах не будет закрыта после завершения задачи *Закрытие уязвимостей* или *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в программах из списка уязвимостей с помощью фильтра.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Пользовательские исправления для уязвимостей в программах сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в программах сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления программ Microsoft и пользовательские исправления для других программ сторонних производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

► *Чтобы выбрать пользовательские исправления для уязвимостей в программах сторонних производителей:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Уязвимости в программах**.

   В рабочей области папки отображается список уязвимостей в программах на устройствах, которые обнаружил Агент администрирования, установленный на них.
2. Выберите уязвимость для которой вы хотите указать пользовательское исправление.
3. В контекстном меню уязвимости выберите пункт **Свойства**.

   Откроется окно свойств уязвимости.

4. В разделе **Пользовательские и другие исправления** нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Удаленная установка → Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости программах сторонних производителей.

6. Нажмите на кнопку **ОК**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в программах. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в программах.

## См. также:

Об обнаружении и закрытии уязвимостей в программах.....519

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Правила установки обновлений

Для закрытия уязвимостей в программах (см. стр. 527) необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, создаете ли вы правило для обновлений программ Microsoft, программ сторонних производителей (программ, производимых поставщиками программного обеспечения, кроме "Лаборатории Касперского" и Microsoft) или всех программ. При создании правила для программ Microsoft или программ сторонних производителей вы можете выбрать программы и версии программ, для которых вы хотите установить обновления. При создании правила для всех программ вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

► Чтобы создать правило для обновления программ:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

2. В окне **Тип правила** выберите **Правило для всех обновлений**.

3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

   - **Набор обновлений для установки**

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на

тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Обновления** выберите обновления для установки:

   - **Устанавливать все подходящие обновления.**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

     Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные программы или чтобы обновить только требуемые программы.

     - **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

       Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

       Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

       Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

       По умолчанию параметр включен.

1. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрывать только уязвимости из списка**

  Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

  Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных программах или чтобы закрыть уязвимости только в требуемых программах.

1. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

► Чтобы создать правило обновления программ Microsoft:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.

2. В окне **Тип правила** выберите **Правило для обновлений Windows Update**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
3. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

► Чтобы создать правило для обновления программ сторонних производителей:

1. В окне **Параметры** мастера создания задачи нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Следуйте далее указаниям мастера.
2. В окне **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Имя** укажите название создаваемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило создастся и отобразится в поле **Задайте правила установки обновлений** мастера создания задачи.

### См. также:

Одобрение и отклонение обновлений программного обеспечения.....493

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей.....516

# Группы программ

В этом разделе описана работа с группами программ, установленных на устройствах.

#### Создание категорий программ

Kaspersky Security Center позволяет создавать категории программ, установленных на устройствах.

Категории программ можно создавать следующими способами:

- Администратор указывает папку, исполняемые файлы из которой попадают в выбранную категорию.
- Администратор указывает устройство, исполняемые файлы с которого попадают в выбранную категорию.
- Администратор задает критерии, по которым программы попадают в выбранную категорию.

Когда категория программ создана, администратор может задать правила для этой категории программ. Правила определяют поведение программ, входящих в указанную категорию. Например, можно запретить или разрешить запуск программ, входящих в категорию.

#### Управление запуском программ на устройствах

Kaspersky Security Center позволяет управлять запуском программ на устройствах в режиме "Список разрешенных". Подробное описание приведено в онлайн-справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm. В режиме "Список разрешенных" на выбранных устройствах разрешен запуск только тех программ, которые входят в указанные категории. Администратор может просматривать результаты статического анализа правил запуска программ на устройствах по каждому пользователю.

### Инвентаризация программного обеспечения, установленного на устройствах

Kaspersky Security Center позволяет выполнять инвентаризацию программного обеспечения на устройствах под управлением Windows. Агент администрирования получает информацию обо всех программах, установленных на устройствах. Информация, полученная в результате инвентаризации, отображается в рабочей области папки **Реестр программ**. Администратор может просматривать подробную информацию о каждой программе, в том числе версию и производителя.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

### Управление группами лицензионных программ

Kaspersky Security Center позволяет создавать группы лицензионных программ. В группу лицензионных программ входят программы, отвечающие критериям, заданным администратором. Администратор может указывать следующие критерии для групп лицензионных программ:

- название программы;
- версия программы;
- производитель;
- тег программы.

Программы, соответствующие одному или нескольким критериям, автоматически попадают в группу. Для создания группы лицензионных программ должен быть задан хотя бы один критерий включения программ в эту группу.

Каждая группа лицензионных программ имеет свой лицензионный ключ. Лицензионный ключ группы лицензионных программ определяет допустимое количество установок для программ, входящих в группу. Если количество установок превысило заданное в лицензионном ключе ограничение, на Сервере администрирования регистрируется информационное событие. Администратор может указать дату окончания действия лицензионного ключа. При наступлении этой даты на Сервере администрирования регистрируется информационное событие.

### Просмотр информации об исполняемых файлах

Kaspersky Security Center получает всю информацию об исполняемых файлах, которые запускались на устройствах с момента установки на них операционной системы. Полученная информация об исполняемых файлах отображается в главном окне программы в рабочей области папки **Исполняемые файлы**.

kaspersky

## В этом разделе



## Сценарий: Управление программами

Вы можете управлять запуском программ на пользовательских устройствах. Вы можете разрешить или запретить запуск программ на управляемых устройствах. Эта функциональность реализуется компонентом Контроль программ. Вы можете управлять программами, установленными на устройствах под управлением Windows или Linux.

Для операционных систем на базе Linux компонент Контроль программ доступен, начиная с версии Kaspersky Endpoint Security 11.2 для Linux.

### Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.

### Этапы

Сценарий использования компонента Контроль программ состоит из следующих этапов:

a. **Формирование и просмотр списка программ на клиентских устройствах**

Этот этап помогает вам определить, какие программы установлены на управляемых устройствах. Вы можете просмотреть список программ и решить, какие программы вы хотите разрешить, а какие запретить, в соответствии с политиками безопасности вашей организации. Ограничения могут быть связаны с политиками информационной безопасности в вашей организации. Вы можете пропустить этот этап, если точно знаете, какие программы установлены на управляемых устройствах.

Инструкции:

Консоль администрирования: Просмотр реестра программ (см. стр. 569).

Kaspersky Security Center 14.2 Web Console: Получение и просмотр списка программ, установленных на клиентских устройствах (см. стр. 1339).

**b. Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации. Вы можете пропустить этот этап, если точно знаете, какие исполняемые файлы установлены на управляемых устройствах.

Инструкции:

Консоль администрирования: Инвентаризация исполняемых файлов (см. стр. 574).

Kaspersky Security Center 14.2 Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах (см. стр. 1340).

**c. Создание категорий программ для программ, используемых в вашей организации**

Проанализируйте списки программ и исполняемых файлов, хранящихся на управляемых устройствах. На основании анализа создайте категории программ. Рекомендуется создать категорию "Рабочие программы", которая охватывает стандартный набор программ, используемых в вашей организации. Если разные группы пользователей используют разные наборы программ в своей работе, для каждой группы пользователей можно создать отдельную категорию программ.

В зависимости от набора критериев для создания категории программ вы можете создавать категории программ трех типов.

Инструкции:

Консоль администрирования: Создание пополняемой вручную категории программ (см. стр. 560), Создание категории программ, в которую входят исполняемые файлы с выбранных устройств (см. стр. 562), Создание категории программ, в которую входят исполняемые файлы из выбранных папок (см. стр. 563)

Kaspersky Security Center 14.2 Web Console: Создание пополняемой вручную категории программ (см. стр. 1342), Создание категории программ, в которую входят исполняемые файлы с выбранных устройств (см. стр. 1345), Создание категории программ, в которую входят исполняемые файлы из выбранных папок (см. стр. 1346).

**d. Настройка компонента Контроль программ в политики Kaspersky Endpoint Security**

Настройте компонент Контроль программ в политике Kaspersky Endpoint Security с использованием категорий программ, которые вы создали на предыдущем этапе.

Инструкции:

Консоль администрирования: Настройка управления запуском программ на клиентских устройствах (см. стр. 567).

Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349).

**e. Включение компонента Контроль программ в тестовом режиме**

Чтобы правила Контроля программ не блокировали программы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля программ и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать программы, запуск которых запрещен правилами Контроля программ, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля программ рекомендуется выполнить следующие действия:

Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.

Изучите события, возникающие в результате тестирования работы компонента Контроль программ.

Инструкции для Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349). Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

f. **Изменение параметров категорий программ компонента Контроль программ**

Если требуется, измените параметры компонента Контроль программ. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль программ, в категорию программ пополняемую вручную.

Инструкции:

Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию программы (см. стр. 565).

Kaspersky Security Center 14.2 Web Console: Добавление исполняемых файлов, связанных с событием, в категорию программы (см. стр. 1351).

g. **Применение правил Контроля программ в рабочем режиме**

После проверки правил Контроля программ и завершения настройки категорий программ вы можете применить правила Контроль программ в рабочем режиме.

Инструкции для Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349). Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

h. **Проверка конфигурации Контроля программ**

Убедитесь, что вы выполнили следующее:

Создали категории программ.

Настроили Контроль программ с использованием категорий программ.

Применили правила Контроля программ в рабочем режиме.

**Результаты**

После завершения сценария, запуск программ на управляемых устройствах контролируется. Пользователи могут запускать только те программы, которые разрешены в вашей организации, и не могут запускать программы, запрещенные в вашей организации.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

## Создание категорий программ для политики Kaspersky Endpoint Security для Windows

Вы можете создать категории программ для политики Kaspersky Endpoint Security для Windows в папке **Категории программ** и в окне **Свойства** политики Kaspersky Endpoint Security для Windows.

► *Чтобы создать категорию программ для политики Kaspersky Endpoint Security в папке **Категории программ**:*

1. В дереве консоли выберите **Дополнительно**→ **Управление программами** → **Категории программ**.

2. В рабочей области папки **Категории программ** нажмите на кнопку **Создать категорию**.

   Запустится мастер создания категории.

3. В окне мастера **Тип категории** выберите тип пользовательской категории:

   - **Пополняемая вручную категория**. Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Укажите устройство, исполняемые файлы которого должны попадать в категорию автоматически.
   - **Категория, в которую входят исполняемые файлы из указанных папок**. Укажите папку, исполняемые файлы которой должны попадать в категорию автоматически.

4. Следуйте далее указаниям мастера.

После завершения мастера создается пользовательская категория программ. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

Также категорию программ можно создать в папке **Политики**.

► *Чтобы создать категорию программ в окне **Свойства** политики Kaspersky Endpoint Security для Windows:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки **Политики** выберите политику Kaspersky Endpoint Security, для которой требуется создать категорию программ.
3. В контекстном меню выберите пункт **Свойства**.
4. В открывшемся окне **Свойства** выберите раздел **Контроль безопасности → Контроль программ**.
5. В разделе **Контроль программ** в раскрывающемся списке **Режим Контроля программ** и **Действие** выберите Список запрещенных или Список разрешенных и нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля программ**, содержащее список категорий.

6. Нажмите на кнопку **Создать**.
7. Введите имя категории и нажмите на кнопку **ОК**.

   Запустится мастер создания категории.

8. В окне мастера **Тип категории** выберите тип пользовательской категории:

   - **Пополняемая вручную категория**. Задайте критерии, по которым исполняемые файлы будут попадать в создаваемую категорию.
   - **Категория, в которую входят исполняемые файлы с выбранных устройств**. Укажите устройство, исполняемые файлы которого должны попадать в категорию автоматически.
   - **Категория, в которую входят исполняемые файлы из указанных папок**. Укажите папку, исполняемые файлы которой должны попадать в категорию автоматически.

9. Следуйте далее указаниям мастера.

После завершения мастера создается пользовательская категория программ. Вы можете просмотреть новую категорию в списке категорий программ.

Категории программ используются компонентом Контроль программ, который входит в состав программы безопасности Kaspersky Endpoint Security для Windows. Компонент Контроль программ позволяет администратору установить ограничения на запуск программ на клиентских устройствах, например, на основании программ, которые входят в выбранную категорию.

kaspersky

См. также:



## Создание пополняемой вручную категории программ

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию программ и использовать ее в настройке компонента Контроль программ.

► *Чтобы создать пополняемую вручную категорию программ:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. Нажмите на кнопку **Создать категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В окне мастера выберите тип пользовательской категории **Пополняемая вручную категория**.
4. На странице мастера **Название категории программ** введите новое имя категории программ.
5. В окне **Настройка условий для включения программ в категорию** нажмите на кнопку **Добавить**.
6. В раскрывающемся списке задайте необходимые вам параметры:
   - **Из списка исполняемых файлов**

     Если выбран этот вариант, программы для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.
   - **Из свойств файла**

     Если выбран этот вариант, можно вручную указать детальные данные исполняемых файлов, которые будут добавлены в пользовательскую категорию программ.
   - **Метаданные файлов папки**

     Укажите папку на клиентском устройстве, которая содержит исполняемые файлы. Метаданные исполняемых файлов, входящих в указанную папку, будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.
   - **Хеши файлов папки**

     Если выбран этот вариант, можно выбрать или создать папку на клиентском устройстве. Хеш файлов, содержащихся в указанной папке, будет передаваться на Сервер администрирования. Программы, имеющие такой же хеш, как и файлы в указанной папке, будут добавлены в пользовательскую категорию программ.
   - **Сертификаты файлов из папки**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, которая содержит исполняемые файлы, подписанные сертификатами. Сертификаты исполняемых файлов считываются и добавляются в условия категории.

Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Метаданные файлов установщика MSI**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика программы будут передаваться на Сервер администрирования. Программы, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию программ.

- **Контрольные суммы файлов msi-инсталлятора программы**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Хеш файлов установщика программы будет передаваться на Сервер администрирования. Программы, у которых хеш файлов установщика MSI совпадает с указанным, будут добавлены в пользовательскую категорию программ.

- **Из KL-категории**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать категорию программ "Лаборатории Касперского". Программы, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию программ.

- **Задайте путь к программе (поддерживаются маски)**

  Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию программ.

- **Выберите сертификат из хранилища сертификатов**

  Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Тип носителя**

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск программы. Программы, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию программ.

7. На странице мастера **Создание категории программ** нажмите на кнопку **Готово**.

Kaspersky Security Center работает с метаданными только из тех файлов, которые содержат цифровую подпись. Невозможно создать категорию на основе метаданных файлов, не содержащих цифровой подписи.

В результате работы мастера будет создана пользовательская категория программ, пополняемая вручную. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

## См. также:

Сценарий:Управление программами .....556

## Создание категории программ, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию программ и использовать ее для настройки компонента Контроль программ.

► *Чтобы создать категорию программ, в которую входят исполняемые файлы с выбранных устройств:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. Нажмите на кнопку **Создать категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория программ, в которую входят исполняемые файлы из выбранных устройств**.
4. На странице мастера **Название категории программ** введите новое имя категории программ.
5. На странице мастера **Параметры** нажмите на кнопку **Добавить**.
6. Выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории программ.
7. Задайте следующие параметры:

   - Алгоритм вычисления хеш-функции

     В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

     SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

     Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

     - Если все экземпляры программ безопасности, установленных в вашей сети, являются версиями программы Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA-256**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
     - Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для

файлов категории.

Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA-256** и флажок **MD5-хеш**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизация данных с хранилищем Сервера администрирования**

Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

По умолчанию параметр выключен.

Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

1. На странице мастера **Фильтр** укажите следующие параметры:

   - **Тип файла**

     В этом разделе вы можете указать тип файла, который используется для создания категории программ.

     **Все файлы**. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

     **Только файлы вне категорий программ**. Для создаваемой категории учитываются только файлы вне категорий программ.

   - **Папки**

В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории программ.

**Все папки**. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

**Указанная папка**. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вы должны указать путь к папке.

1. На странице мастера **Создание категории программ** нажмите на кнопку **Готово**.

После завершения мастера создается пользовательская категория программ. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

## Создание категории программ, в которую входят исполняемые файлы из указанных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию программ и использовать ее для настройки компонента Контроль программ.

► *Чтобы создать категорию программ, в которую входят исполняемые файлы из указанных папок:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. Нажмите на кнопку **Создать категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На странице мастера **Тип категории** выберите тип пользовательской категории **Категория программ, в которую входят исполняемые файлы из указанных папок**.
4. На странице мастера **Название категории программ** введите новое имя категории программ.
5. На странице мастера **Папка хранилища** нажмите на кнопку **Обзор**.
6. Укажите папку, исполняемые файлы которой будут использоваться для создания категории программ.
7. Настройте следующие параметры:
   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию программ включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль программ регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.
   - **Включать в категорию данные о скриптах**

     В категорию программ включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.
   - Алгоритм вычисления хеш-функции: **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

     В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

     SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

     Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

     - Если все экземпляры программ безопасности, установленных в вашей сети, являются версиями программы Kaspersky Endpoint Security 10 Service Pack 2 для

Windows и выше, установите флажок **SHA-256**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.

Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA-256** и флажок **MD5-хеш**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, программа периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

8. На странице мастера **Создание категории программ** нажмите на кнопку **Готово**.

После завершения мастера создается пользовательская категория программ. Просмотреть созданную категорию можно в списке категорий в рабочей области папки **Категории программ**.

## Добавление исполняемых файлов, связанных с событием, в категорию программы

Вы можете добавить исполняемые файлы, связанные с событиями **Запуск программы запрещен** и **Запуск программы запрещен в тестовом режиме**, в существующую категорию программ, пополняемую вручную, или в новую категорию программ.

► *Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль программ, в категорию программ:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. На закладке **События** выберите нужное вам событие.
4. В контекстном меню события выберите пункт **Добавить в категорию**.

5. В окне **Выберите категорию программ** настройте необходимые вам параметры:

   Выберите один из следующих вариантов:

   - **Создать категорию программ**

     Выберите этот вариант, если вы хотите создать категорию программ.

     По кнопке **ОК** запустите мастер создания пользовательской категории. В результате работы мастера будет создана категория с указанными параметрами.

     По умолчанию вариант не выбран.

   - **Добавить правила в указанную категорию**

     Выберите этот вариант, если необходимо добавить правила в существующую категорию программ. Выберите необходимую категорию в списке категорий программ.

     По умолчанию этот вариант выбран.

   В блоке **Тип правила** выберите параметры:

   - **Добавить в категорию**

     Выберите этот вариант, если необходимо добавить правила в условия категории программ.

     По умолчанию этот вариант выбран.

   - **Исключить из категории**

     Выберите этот вариант, если вы хотите добавить правила в исключения категории программ.

   В блоке **Тип информации о файле** выберите один из параметров:

   - **Данные сертификата или SHA-256 для файлов без сертификата**

     Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

     Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

     Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

     По умолчанию выбран этот вариант.

   - **Данные сертификата (файлы без сертификата пропускаются)**

     Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

- **Только SHA-256 (файлы без SHA-256 пропускаются)**

  Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

- **MD5 (устаревший режим, только для версий Kaspersky Endpoint Security 10 Service Pack 1)**

  Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

  Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

6. Нажмите на кнопку **ОК**.

## См. также:

Сценарий:Управление программами .....556

## Настройка управления запуском программ на клиентских устройствах

Категоризация программ позволяет оптимизировать процесс управления запуском программ на устройствах. Вы можете создать категорию программ и настроить компонент Контроль программ политики так, что на устройствах, на которых применена эта политика, будут запускаться только программы из указанной категории. Например, вы создали категорию, которая содержит программы *Программа_1* и *Программа_2*. После добавления этой категории в политику, на устройствах, к которым применена эта политика, будет разрешен запуск только двух программ: *Программа_1* и *Программа_2*. Если пользователь попытается запустить программу, которая не входит в категорию, например, *Программу_3*, то запуск такой программы будет заблокирован. Пользователю будет отображено сообщение о том, что запуск *Программы_3* запрещен в соответствии с правилом Контроля программ. Вы можете создать автоматически пополняемую категорию на основе различных критериев, входящих в указанную папку. В этом случае файлы будут автоматически добавляться в категорию из указанной папки. Исполняемые файлы программ копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию.

► *Чтобы настроить управление запуском программ на клиентских устройствах:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Категории программ**.
2. В рабочей области папки **Категории программ** создайте категории программ (см. стр. 558), запуском которых вы хотите управлять.
3. Чтобы создать политику (см. стр. 430) для программы Kaspersky Endpoint Security для Windows, в папке **Управляемые устройства** на закладке **Политики** нажмите на кнопку Новая политика и следуйте указаниям мастера.

Если такая политика уже существует, этот шаг можно пропустить. Управление запуском программ в указанной категории можно настроить в параметрах этой политики. Созданная политика отображается в папке **Управляемые устройства** на закладке **Политики**.

4. В контекстном меню политики для программы Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики Kaspersky Endpoint Security для Windows.

5. В окне свойств политики Kaspersky Endpoint Security для Windows, в разделе **Контроль безопасности → Контроль программ** установите флажок **Контроль программ**.

6. Нажмите на кнопку **Добавить**.

   Откроется окно **Правило Контроля программ**.

7. В окне **Правило Контроля программ** в раскрывающемся списке **Категория** выберите категорию программ, на которую будет распространяться правило запуска. Настройте параметры правила запуска для выбранной категории программ.

   Для программ версий Kaspersky Endpoint Security для Windows 10 Service Pack 2 и выше категории, созданные по критерию MD5-хеша исполняемого файла, программы не отображаются.

   Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для программ версий ниже Kaspersky Endpoint Security для Windows 10 Service Pack 2. Это может привести к сбою программы.

   Подробные инструкции по настройке правил контроля приведены в онлайн-справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm.

8. Нажмите на кнопку **ОК**.

Запуск программ на устройствах, входящих в указанную категорию, будет выполняться согласно созданному правилу. Созданное правило отображается в окне свойств политики Kaspersky Endpoint Security для Windows в разделе **Контроль программ**.

## См. также:

Сценарий:Управление программами .....556

## Просмотр результатов статического анализа правил запуска исполняемых файлов

► *Чтобы просмотреть информацию о том, запуск каких исполняемых файлов запрещен пользователям:*

1. В дереве консоли в папке **Управляемые устройства** выберите закладку **Политики**.
2. В контекстном меню политики для программы Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.

   Откроется окно свойств политики программы.

3. В окне свойств политики выберите раздел **Контроль безопасности**, а затем подраздел **Контроль программ**.
4. Нажмите на кнопку **Статический анализ**.

   Откроется окно **Анализ списка прав доступа**. В левой части окна отображается список пользователей, основанный на данных Active Directory.

5. Выберите в списке пользователя.

В правой части окна отобразятся категории программ, назначенные этому пользователю.

6. Чтобы просмотреть исполняемые файлы, запуск которых запрещен пользователю, в окне **Анализ списка прав доступа** нажмите на кнопку **Просмотреть файлы**.

   Откроется окно, в котором отображается список исполняемых файлов, запуск которых запрещен пользователю.

7. Чтобы просмотреть список исполняемых файлов, входящих в категорию, выберите категорию программ и нажмите на кнопку **Просмотреть файлы категории**.

   В открывшемся окне отображается список исполняемых файлов, входящих в категорию программ.

См. также:

Сценарий:Управление программами .....556

## Просмотр реестра программ

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых устройствах.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных программах из реестра Windows.

Получение информации об установленных программах поддерживается только для операционных систем Microsoft Windows.

► *Чтобы просмотреть реестр установленных на клиентских устройствах программ,*

В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Реестр программ**.

В рабочей области папки **Реестр программ** отображается список программ, установленных на клиентских устройствах и Сервере администрирования.

Вы можете просмотреть подробную информацию о любой программе, выбрав в контекстном меню этой программы пункт **Свойства**. В окне свойств программы отображается общая информация о программе и информация об исполняемых файлах программы, а также список устройств, на которых установлена программа.

В контекстном меню любой программы вы можете:

- добавить эту программу в категорию программ;
- назначить тег программе;
- экспортировать список программ в файлы форматов CSV или TXT;
- просмотреть свойства программы, например имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлена программа, список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

Для просмотра программ, удовлетворяющих определенным критериям, вы можете воспользоваться полями фильтрации в рабочей области папки **Реестр программ**.

В окне свойств выбранного устройства (см. стр. 742) в разделе **Реестр программ** вы можете просмотреть список программ, установленных на устройстве.

#### Генерирование отчета об установленных программах

В рабочей области папки **Реестр программ** вы также можете нажать на кнопку **Просмотреть отчет об установленных программах**, чтобы сгенерировать отчет, содержащий информацию об установленных программах, включая количество устройств, на которых установлена каждая программа. Отчет, который открывается на странице **Отчет об установленных программах**, содержит информацию о программах "Лаборатории Касперского" и о программах сторонних производителей. Если вам нужна информация только о программах "Лаборатории Касперского", установленных на клиентских устройствах, в списке **Сводная информация** выберите "Лаборатория Касперского".

Информация о программах "Лаборатории Касперского" и других производителей на устройствах, подключенных к подчиненным и виртуальным Серверам администрирования, также хранится в реестре программ главного Сервера администрирования. После добавления данных с подчиненных и виртуальных Серверов нажмите на кнопку **Просмотреть отчет об установленных программах**, и на открывшейся странице **Отчет об установленных программах** вы можете просмотреть эту информацию.

► *Чтобы добавить информацию с подчиненных и виртуальных Серверов администрирования в отчет об установленных программах:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. На закладке **Отчеты** выберите **Отчет об установленных программах**.
4. В контекстном меню отчета выберите пункт **Свойства**.

   Откроется окно **Свойства: Отчет об установленных программах**.
5. В разделе **Иерархия Серверов администрирования** установите флажок **Использовать данные с подчиненных и виртуальных Серверов администрирования**.
6. Нажмите на кнопку **ОК**.

В результате информация с подчиненных и виртуальных Серверов администрирования будет включена в **Отчет об установленных программах**.

### См. также:


Мониторинг установки и удаления программ ..... 617

Сценарий:Управление программами ..... 556

Основной сценарий установки ..... 92


## Изменение времени начала инвентаризации программного обеспечения

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Windows.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агент администрирования автоматически получает информацию об установленных программах из реестра Windows.

Чтобы сохранить ресурсы устройства, по умолчанию Агент администрирования начинает получать информацию об установленных программах через 10 минут после запуска службы Агента администрирования.

► *Чтобы изменить время начала инвентаризации программного обеспечения устройства после запуска службы Агента администрирования:*

1. Откройте системный реестр устройства, на котором установлен Агент администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
3. Для ключа KLINV_INV_COLLECTOR_START_DELAY_SEC установите нужное вам значение в секундах.

   По умолчанию указано значение 600 секунд.
4. Перезапустите службу Агента администрирования.

В результате время начала инвентаризации программного обеспечения после запуска службы Агента администрирования изменится.

## См. также:

Сценарий:Управление программами .....556

## Об управлении лицензионными ключами программ сторонних производителей

Kaspersky Security Center позволяет отслеживать использование лицензионных ключей для программ сторонних производителей, установленных на управляемых устройствах. Список программ, для которых вы можете отслеживать использование лицензионного ключа, берется из реестра программ (см. стр. 569). Для каждого лицензионного ключа вы можете указать и отслеживать нарушение следующих ограничений:

- Максимальное количество устройств, на которых может быть установлена программа, использующая этот лицензионный ключ.
- Дата окончания срока действия лицензионного ключа.

Kaspersky Security Center не проверяет, указали ли вы реальный лицензионный ключ. Вы можете отслеживать только те ограничения, которые вы указали. В случае нарушения одного из ограничений, которые вы накладываете на лицензионный ключ, Сервер администрирования регистрирует событие информационное (см. стр. 642), предупреждающее (см. стр. 631) или отказ функционирования (см. стр. 625).

Лицензионные ключи привязаны к группам программ. Группа программ – это группа программ сторонних производителей, которые вы объединяете на основе одного критерия или нескольких критериев. Вы можете определять программы по имени программы, версии программы, поставщику и тегу. Программа добавляется в группу, если выполняется хотя бы один из критериев. К каждой группе программ вы можете привязать

несколько лицензионных ключей, но каждый лицензионный ключ может быть привязан только к одной группе программ.

Также вы можете использовать отчет о состоянии групп лицензионных программ для отслеживания использования лицензионных ключей. В этом отчете представлена информация о текущем состоянии групп лицензионных программ, в том числе:

- Количество установок лицензионных ключей на каждую группу программ.
- Количество используемых лицензионных ключей и свободных лицензионных ключей.
- Список лицензионных программах, установленных на управляемых устройствах.

Инструменты для управления лицензионными ключами программ сторонних производителей расположены в папке **Учет сторонних лицензий** (**Дополнительно → Управление программами → Учет сторонних лицензий**). В этой папке вы можете создавать группы программ (см. стр. 572), добавлять лицензионные ключи (см. стр. 573) и формировать отчет о состоянии групп лицензионных программ.

Инструменты для управления лицензионными ключами программ сторонних производителей доступны, только если вы включили параметр Системное администрирование в окне **Настройка интерфейса** (см. стр. 322).

## Создание групп лицензионных программ

► *Чтобы создать группу лицензионных программ:*

1. В дереве консоли в папке **Дополнительно → Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. По кнопке **Добавить группу лицензионных программ** запустите мастер добавления группы лицензионных программ.

   Мастер добавления группы лицензионных программ запущен.
3. На шаге **Информация о группе лицензионных программ** укажите, какие программы вы хотите включить в группу программ:
   - **Название группы лицензионных программ**
   - **Отслеживать нарушение ограничений**
   - **Критерии включения обнаруженных программ в эту группу лицензионных программ**
4. На шаге **Введите данные о имеющихся лицензионных ключах** укажите лицензионные ключи, которые вы хотите отслеживать. Выберите параметр **Контролировать нарушение заданных лицензионных ограничений** и добавьте лицензионные ключи:
   a. Нажмите на кнопку **Добавить**.
   b. Выберите лицензионный ключ, который нужно добавить, и нажмите на кнопку **ОК**. Если необходимый лицензионный ключ отсутствует в списке, нажмите на кнопку **Добавить** и укажите свойства лицензионного ключа (см. стр. 573).
5. На шаге **Добавление группы лицензионных программ** нажмите на копку **Готово**.

Создается группа лицензионных программ, которая отображается в папке **Учет сторонних лицензий**.

### См. также:

Сценарий:Управление программами .....556

## Управление лицензионными ключами для групп лицензионных программ

► *Чтобы создать лицензионный ключ для группы лицензионных программ:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. В рабочей области папки **Учет сторонних лицензий** нажмите на кнопку **Управлять ключами лицензионных программ**

   Откроется окно **Управление лицензионными ключами лицензионных программ**.
3. В окне **Управление лицензионными ключами лицензионных программ** нажмите на кнопку **Добавить**.

   Откроется окно **Ключ**.
4. В окне **Лицензионный ключ** укажите свойства лицензионного ключа и ограничения, которые этот лицензионный ключ накладывает на группу лицензионных программ.
   - **Имя**. Название лицензионного ключа.
   - **Комментарий**. Примечания к выбранному лицензионному ключу.
   - **Ограничение**. Количество устройств, на которых может быть установлена программа, использующая этот лицензионный ключ.
   - **Срок действия**. Дата окончания срока действия лицензионного ключа.

Созданные лицензионные ключи отображаются в окне **Управление лицензионными ключами лицензионных программ**.

► *Чтобы применить лицензионный ключ к группе лицензионных программ:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Учет сторонних лицензий**.
2. В папке **Учет сторонних лицензий** выберите группу лицензионных программ, к которой вы хотите применить лицензионный ключ.
3. В контекстном меню группы лицензионных программ выберите пункт **Свойства**.

   Откроется окно свойств группы лицензионных программ.
4. В окне свойств группы лицензионных программ в разделе **Лицензионные ключи** выберите вариант **Контролировать нарушение заданных лицензионных ограничений**.
5. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор лицензионного ключа**.
6. В окне **Выбор лицензионного ключа** выберите лицензионный ключ, который вы хотите применить к группе лицензионных программ.
7. Нажмите на кнопку **ОК**.

Ограничения для группы лицензионных программ, указанные в лицензионном ключе, будут распространены на выбранную группу лицензионных программ.

### См. также:

Сценарий:Управление программами .....556

kaspersky

## Инвентаризация исполняемых файлов

Инвентаризацию исполняемых файлов на клиентских устройствах можно выполнить с помощью задачи инвентаризации. Инвентаризация исполняемых файлов реализована в программе Kaspersky Endpoint Security для Windows.

Количество исполняемых файлов, получаемых от одного устройства, не может превышать 150 000. При достижении этого ограничения Kaspersky Security Center не получит новые файлы.

Прежде чем начать, включите уведомления о запуске программ в политике Kaspersky Endpoint Security и в политике Агента администрирования, чтобы можно было передавать данные на Сервер администрирования.

► *Чтобы включить уведомления о запуске программ:*

- Откройте параметры политики Kaspersky Endpoint Security и выполните следующие действия:
  1. Перейти к **Общие параметры** → **Отчеты и хранилища**.
  2. В разделе **Передача данных на Сервер администрирования**, установите флажок **О запускаемых программах**.
  3. Сохраните изменения.
- Откройте параметры политики Агента администрирования и выполните следующие действия:
  1. Перейдите в раздел **Хранилища**.
  2. Установите флажок **Информация об установленных программах**.
  3. Сохраните изменения.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:*

1. В дереве консоли выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи.
3. В окне мастера **Выбор типа задачи** выберите тип задачи **Kaspersky Endpoint Security**, затем подтип задачи **Инвентаризация** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате работы мастера создается задача инвентаризации для Kaspersky Endpoint Security. Созданная задача отображается в списке задач в рабочей области папки **Задачи**.

Список исполняемых файлов, обнаруженных на устройствах в результате выполнения инвентаризации, отображается в рабочей области папки **Исполняемые файлы**.

При выполнении инвентаризации программа обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML-файлы.

### См. также:

Сценарий:Управление программами ..... 556

### Просмотр информации об исполняемых файлах

► *Чтобы просмотреть список всех исполняемых файлов, обнаруженных на клиентских устройствах,*

в дереве консоли в папке **Управление программами** выберите вложенную папку **Исполняемые файлы**.

В рабочей области папки **Исполняемые файлы** отображается список исполняемых файлов, которые запускались на устройствах с момента установки операционной системы или были обнаружены в процессе работы задачи инвентаризации Kaspersky Endpoint Security для Windows.

Для просмотра данных об исполняемых файлах, удовлетворяющих определенным критериям, вы можете воспользоваться фильтрацией.

► *Чтобы просмотреть свойства исполняемого файла,*

в контекстном меню файла выберите пункт **Свойства**.

Откроется окно, содержащее информацию об исполняемом файле, а также список устройств, на которых присутствует исполняемый файл.

См. также:

Сценарий:Управление программами .....556

# Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

- Индикаторы

  В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов.

- Статистика

  Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей.

- Отчеты

  Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

- События

  Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

  - Уровень важности: **Критические события**, **Сбой**, **Предупреждение** и **Информационные события**.

- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 14.2 Web Console.

## В этом разделе



# Сценарий: Мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

**Предварительные требования**

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

**Этапы**

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

**a.** Настройка переключения статусов устройств

Ознакомьтесь с параметрами, определяющими присвоение статусов устройствам в зависимости от конкретных условий. Изменяя эти параметры (см. стр. 727), вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*.

При настройке переключения статусов устройств убедитесь, что новые параметры не конфликтуют с политиками информационной безопасности вашей организации и что вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

**b.** Настройка параметров уведомлений о событиях на клиентских устройствах

Настройте уведомления (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах (см. стр. 316), в соответствии с потребностями вашей организации.

**c.** Изменение ответа вашей сети безопасности на событие Вирусная атака

Чтобы настроить ответ сети на новые события, вы можете изменить пороговые значения (см. стр. 687) в свойствах Сервера администрирования. Вы также можете создать более строгую политику (см.

стр. 432), которая будет активирована, или создать задачу (см. стр. 413), которая будет запускаться при возникновении этого события.

**d.** Работа со статистической информацией

Настройте отображение статистики (см. стр. 594) в соответствии с потребностями вашей организации.

**e.** Просмотр состояния безопасности сети вашей организации

Чтобы проверить состояние безопасности сети вашей организации, вы можете выполнить любое из следующих действий:

В рабочей области узла **Сервер администрирования**, на закладке **Статистика** откройте закладку второго уровня (страницу) **Состояние защиты** и просмотрите информационную панель **Статус постоянной защиты**.

Генерация и просмотр отчета**Отчет о состоянии защиты** (см. стр. 588).

Генерация и просмотр отчета **Отчет об ошибках** (см. стр. 588).

**f.** Нахождение незащищенных клиентских устройств

Чтобы найти незащищенные клиентские устройства, перейдите в рабочую область узла **Сервер администрирования**, на закладке **Статистика** откройте закладку второго уровня (страницу) **Статус защиты** и просмотрите информационную панель **История обнаружения новых устройств в сети**. Также можно создать и просмотреть отчет **Отчет о развертывании защиты** (см. стр. 588).

**g.** Проверка защиты клиентских устройств

Чтобы проверить защиту клиентских устройств, перейдите в рабочую область узла **Сервер администрирования**, на закладке **Статистика** откройте **Развертывание** или закладку второго уровня (страницу) **Статистика угроз** и просмотрите соответствующие информационные панели. Вы также можете начать и просматривать выборку событий **Критические события** (см. стр. 601).

**h.** Оценка и ограничение загрузки событий в базу данных

Информация о событиях, которые возникают во время работы управляемых программ, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Чтобы оценить загрузку событий в базе данных, рассчитайте место в базе данных. Вы также можете ограничить максимальное количество событий (см. стр. 410) чтобы избежать переполнения базы данных.

**i.** Просмотр информации о лицензии

Чтобы просмотреть информацию о лицензии, перейдите в рабочую область узла **Сервер администрирования**, на закладке **Статистика** откройте закладку второго уровня (страницу) **Развертывание** и просмотрите информационную панель **Используемые лицензионные ключи**. Также можно создать и просмотреть отчет **Отчет об использовании лицензионных ключей** (см. стр. 588).

**Результаты**

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

kaspersky

# Мониторинг цветовых индикаторов и зарегистрированных событий в Консоли администрирования

В Консоли администрирования можно быстро оценить текущее состояние Kaspersky Security Center и управляемых устройств с помощью цветовых индикаторов. Индикаторы отображаются в рабочей области узла **Сервер администрирования** на закладке **Мониторинг**. На закладке имеется шесть информационных блоков с цветовыми индикаторами и зарегистрированными событиями. Цветной индикатор – это цветная вертикальная полоса на левой стороне панели. Каждый блок с индикатором отвечает за отдельную функциональную область Kaspersky Security Center (см. таблицу ниже).

*Таблица 56. Области ответственности цветовых индикаторов в Консоли администрирования*

| Название панели | Область ответственности цветового индикатора |
|---|---|
| **Развертывание** | Установка Агента администрирования и программ безопасности на устройства сети организации. |
| **Структура управления** | Структура групп администрирования. Сканирование сети. Правила перемещения устройств. |
| **Параметры защиты** | Функции программы безопасности: состояние защиты, поиск вредоносного ПО. |
| **Обновление** | Обновления и патчи. |
| **Мониторинг** | Состояние защиты. |
| **Сервер администрирования** | Функции и свойства Сервера администрирования. |

Индикатор может быть одного из пяти цветов (см. таблицу ниже). Цвет индикатора зависит от текущего состояния Kaspersky Security Center и от зарегистрированных событий.

*Таблица 57. Цветовые кодировки индикаторов*

| Состояние | Цвет индикатора | Значение цвета индикатора |
|---|---|---|
| Информационное | Зеленый | Вмешательство администратора не требуется. |
| Предупреждение | Желтый | Требуется вмешательство администратора. |
| Предельный | Красный | Имеются серьезные проблемы. Требуется вмешательство администратора для их решения. |
| Информационное | Голубой | Зарегистрированы события, не связанные с угрозами для безопасности управляемых устройств. |
| Информационное | Серый | Информация о событиях недоступна или еще не получена. |

Цель администратора поддерживать индикаторы в состоянии "зеленый" на всех информационных панелях закладки **Мониторинг**.

На информационных панелях также отображаются зарегистрированные события, влияющие на цветовые индикаторы, и состояние Kaspersky Security Center (см. таблицу ниже).

*Таблица 58. Название, описание и цвет индикатора зарегистрированных событий*

| Цвет индикатора | Отображаемое имя типа события | Тип события | Описание |
|---|---|---|---|
| Красный | **Количество устройств, на которых срок действия лицензии истек: %1.** | IDS_AK_STATUS_LIC_EXPAIRED | События этого типа возникают, если срок действия коммерческой лицензии (см. стр. 342) окончен.<br>Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии.<br>После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (на стр. 356).<br>Чтобы продолжить использование Kaspersky Security Center, продлите срок действия коммерческой лицензии. |
| Красный | **Устройств с не запущенной программой безопасности: %1** | IDS_AK_STATUS_AV_NOT_RUNNING | События этого типа возникают, когда программа безопасности, установленная на устройстве, не запущена.<br>Убедитесь, что на устройстве запущена программа Kaspersky Endpoint Security. |

| Цвет индикатора | Отображаемое имя типа события | Тип события | Описание |
|---|---|---|---|
| Красный | **Устройств с выключенной защитой: %1** | IDS_AK_STATUS_RTP_NOT_RUNNING | События такого типа возникают, когда программа безопасности на устройстве отключена больше указанного времени.<br>Проверьте текущий статус постоянной защиты (см. стр. 742) на устройстве и убедитесь, что все необходимые вам компоненты защиты включены. |
| Красный | **Обнаружена уязвимость в программном обеспечении на устройствах.** | IDS_AK_STATUS_VULNERABILITIES_FOUND | События этого типа происходят, когда задача *Поиск уязвимостей и требуемых обновлений* обнаружила уязвимости с указанным уровнем критичности (см. стр. 550) в программах, установленных на устройстве.<br>Проверьте список доступных обновлений (см. стр. 492) в подпапке **Обновления программного обеспечения**, вложенной в папку **Управление программами**. Эта папка содержит список полученных Сервером администрирования обновлений программ Microsoft и других производителей программного обеспечения, которые могут быть распространены на устройства.<br>Просмотрите информацию о доступных обновлениях и установите их на устройство (см. стр. 501). |

| Цвет индикатора | Отображаемое имя типа события | Тип события | Описание |
|---|---|---|---|
| Красный | **На Сервере администрирования зарегистрированы критические события.** | IDS_AK_STATUS_EVENTS_OCCURED | События этого типа возникают при обнаружении критических событий Сервера администрирования.<br>Проверьте список событий (см. стр. 601), хранящихся на Сервере администрирования, а затем последовательно исправьте критические события. |
| Красный | **На Сервере администрирования зарегистрированы ошибки в событиях.** | IDS_AK_STATUS_ERROR_EVENTS_OCCURED | События этого типа возникают при регистрации непредвиденных ошибок на стороне Сервера администрирования.<br>Проверьте список событий (см. стр. 601), хранящихся на Сервере администрирования, а затем последовательно исправьте критические события. |
| Красный | **Потеряно соединение с устройствами: %1.** | IDS_AK_STATUS_ADM_LOST_CONTROL1 | События этого типа возникают при потере соединения между Сервером администрирования и устройством.<br>Просмотрите список отключенных устройств и попробуйте подключить их снова. |
| Красный | **Устройств, которые давно не соединялись с Сервером администрирования: %1.** | IDS_AK_STATUS_ADM_NOT_CONNECTED1 | События этого типа возникают, когда устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.<br>Убедитесь, что устройство включено и запущен Агент администрирования. |

| Цвет индикатора | Отображаемое имя типа события | Тип события | Описание |
|---|---|---|---|
| Красный | **Есть %1 устройств со статусом отличным от "OK".** | IDS_AK_STATUS_HOST_NOT_OK | События этого типа происходят, когда статус устройства *OK*, подключенного к Серверу администрирования, меняется на *Критический* или *Предупреждение*.<br>Устранить неполадку можно с помощью утилиты удаленной диагностики Kaspersky Security Center (см. стр. 735). |
| Красный | **Базы устарели: %1 устройств.** | IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED | События этого типа возникают, когда антивирусные базы на устройстве не обновлялись в течение заданного интервала времени.<br>Следуйте инструкциям, чтобы обновить антивирусные базы "Лаборатории Касперского" (см. стр. 461). |
| Красный | **Устройств, на которых давно не осуществлялась проверка обновлений Центра обновления Windows: %1.** | IDS_AK_STATUS_WUA_DATA_OBSOLETE | События этого типа возникают, когда задача *Синхронизация обновлений Windows Update* не выполнялась больше указанного времени.<br>Следуйте инструкциям, чтобы синхронизировать обновления из Центра обновления Windows Update с Сервером администрирования (см. стр. 494). |

| Цвет индикатора | Отображаемое имя типа события | Тип события | Описание |
|---|---|---|---|
| Красный | **Для Kaspersky Security Center требуется установка плагинов: %1.** | IDS_AK_STATUS_PLUGINS_REQUIRED2 | События этого типа возникают, когда вам нужно установить дополнительные плагины для программ "Лаборатории Касперского".<br>Загрузите и установите необходимые плагины управления для программы "Лаборатории Касперского" с веб-сайта Службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.com/9333. |

# Работа с отчетами, статистикой и уведомлениями

В этом разделе представлена информация о работе с отчетами, статистикой и выборками событий и устройств в Kaspersky Security Center, а также о настройке параметров уведомлений Сервера администрирования.

## В этом разделе



## Работа с отчетами

Отчеты в Kaspersky Security Center содержат информацию о состоянии управляемых устройств. Отчеты формируются на основании информации, хранящейся на Сервере администрирования. Вы можете создавать отчеты для следующих объектов:

- для выборок устройств, созданных по определенным параметрам;
- для групп администрирования;
- для наборов устройств из разных групп администрирования;
- для всех устройств в сети (в отчете о развертывании).

В программе есть набор стандартных шаблонов отчетов. Предусмотрена также возможность создавать пользовательские шаблоны отчетов. Отчеты отображаются в главном окне программы, в папке дерева консоли **Сервер администрирования**.

## В этом разделе



## Создание шаблона отчета

► *Чтобы создать шаблон отчета:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Нажмите на кнопку **Новый шаблон отчета**.

   В результате запустится мастер создания шаблона отчета. Следуйте далее указаниям мастера.

После окончания работы мастера сформированный шаблон отчета будет добавлен в состав выбранной папки **Сервер администрирования** дерева консоли. Этот шаблон можно использовать для создания и просмотра отчетов.

## Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

► *Чтобы просмотреть и изменить свойства шаблона отчета:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.

   Также вы можете сначала создать отчет, а затем нажать на кнопку **Открыть свойства шаблона отчета** или на кнопку **Настроить графы отчета**.
5. В открывшемся окне вы можете изменить свойства шаблона отчета. Свойства каждого отчета могут содержать только некоторые из разделов, описанных ниже.
   - Раздел **Общие**:
     - Название шаблона отчета
     - **Максимальное число отображаемых записей**

Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Поля отчета** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

По умолчанию параметр включен. По умолчанию указано значение 1000.

- **Версия для печати**

  Отчет оптимизирован для печати: добавлены пробелы, между некоторыми значениями для лучшей визуальной доступности.

  По умолчанию параметр включен.

- Раздел **Поля отчета**.

  Выберите поля, которые будут отображаться в отчете и порядок этих полей. Также настройте, должна ли информация в отчете сортироваться и фильтроваться по каждому из полей.

- Раздел **Период**.

  Измените отчетный период. Доступные значения:

  - между двумя указанными датами;
  - от указанной даты до даты создания отчета;
  - от даты создания отчета минус указанное количество дней до даты создания отчета.

- Разделы **Группа**, **Выборка устройств**, или **Устройства**.

  Измените набор клиентских устройств, для которых создается отчет. В зависимости от параметров, указанных при создании шаблона, может присутствовать только один из этих разделов.

- Раздел **Параметры**.

  Измените параметры отчета. Набор параметров зависит от конкретного отчета.

- Раздел **Безопасность**. **Наследовать параметры Сервера администрирования или родительской группы**

  Если этот параметр включен, параметры отчета наследуются с Сервера администрирования.

  Если этот параметр выключен, вы можете настроить параметры отчета. Вы можете назначить роль пользователю или группе пользователей (см. стр. 797) или назначить права пользователю или группе пользователей (см. стр. 798), применительно к отчету.

  По умолчанию параметр включен.

Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. стр. 685).

- Раздел **Иерархия Серверов администрирования**:
  - **Использовать данные с подчиненных и виртуальных Серверов администрирования**

    Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

    Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

    По умолчанию параметр включен.

  - **До уровня вложенности**

    Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

    По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию подчиненных Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

  - **Период ожидания данных (мин.)**
  - **Кешировать данные с подчиненных Серверов администрирования**

    Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

    Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

    Включение этой опции позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

    По умолчанию параметр выключен.

  - **Период обновления данных в кеше (ч)**

    Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

    По умолчанию указано значение 0.

  - **Передавать подробную информацию с подчиненных Серверов администрирования**

    В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

    Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все

данные в одном отчете.

Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

По умолчанию параметр выключен.

## Расширенный формат фильтра в шаблонах отчета

В программе Kaspersky Security Center вы можете применить расширенный формат фильтра к шаблонам отчета. Расширенный формат фильтра обеспечивает большую гибкость по сравнению с форматом по умолчанию. Вы можете создавать сложные условия фильтрации, используя набор фильтров, которые будут применяться к отчету с помощью логического оператора OR при создании отчета, как показано ниже:

Фильтр[1](Поле[1] AND Поле[2]... AND Полем[n]) OR Фильтр[2](Поле[1] AND Поле[2]... AND Поле[n]) OR... Фильтр[n](Поле[1] AND Поле[2]... AND Поле[n])

Кроме того, с помощью расширенного формата фильтра вы можете установить значение временного интервала в формате относительного времени (например, с помощью условия "За последние N дней") для определенных полей фильтра. Доступность и набор условий временного интервала зависят от типа шаблона отчета.

### В этом разделе



*Конвертация фильтра в расширенный формат*

Расширенный формат фильтра для шаблонов отчета поддерживается только в версии Kaspersky Security Center 12 и выше. После конвертации фильтра по умолчанию в расширенный формат, шаблон отчета становится несовместимым с Серверами администрирования вашей сети, на которых установлены более ранние версии Kaspersky Security Center. Информация с этих Серверов администрирования не будет получена для отчета.

► *Чтобы конвертировать из формата по умолчанию в расширенный формат:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В списке шаблонов отчетов выберите требуемый шаблон отчета.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В открывшемся окне свойств выберите раздел **Поля отчета**.
6. На закладке **Детальные данные** перейдите по ссылке **Конвертировать фильтр**.
7. В появившемся окне нажмите на кнопку **ОК**.

Конвертация в расширенный формат фильтра необратима для шаблона отчета, к которому он применяется. Если вы случайно перешли по ссылке **Конвертировать фильтр**, вы можете отменить изменения, нажав на кнопку **Отмена** в окне свойств шаблона отчета.

8. Чтобы применить изменения, закройте окно свойств шаблона отчета, нажав на кнопку **ОК**.

   Когда снова откроется окно свойств шаблона отчета, отобразится новый доступный раздел **Фильтры**. В этом разделе вы можете настроить расширенный формат фильтра (см. стр. 588).

*Настройка расширенного фильтра*

► *Чтобы настроить параметры расширенного фильтра в шаблоне отчета:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. В списке шаблонов отчетов выберите шаблон отчета, который ранее был конвертирован в расширенный формат фильтра (см. стр. 587).
4. В контекстном меню выбранного шаблона отчета выберите пункт **Свойства**.
5. В отобразившемся окне свойств выберите раздел **Фильтры**.

   Раздел **Фильтры** не отображается, если шаблон отчета не был ранее конвертирован в расширенный формат фильтра (см. стр. 587).

   В окне свойства шаблона отчета в разделе **Фильтры** вы можете просмотреть и изменить список примененных фильтров к отчету. Каждый фильтр в списке имеет уникальное имя и представляет собой набор фильтров для соответствующих полей в отчете.
6. Откройте окно свойств фильтра одним из следующих способов:
   - Чтобы создать фильтр, нажмите на кнопку **Добавить**.
   - Чтобы изменить существующий фильтр, выберите необходимый фильтр и нажмите на кнопку **Изменить**.
7. В открывшемся окне выберите и укажите значения обязательных полей фильтра.
8. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно.

   Если вы создаете фильтр, имя фильтра должно быть указано в поле **Имя фильтра**, прежде чем нажать на кнопку **ОК**.
9. Закройте окно свойств шаблона отчета, нажав на кнопку **ОК**.

   Расширенный фильтр в шаблоне отчета настроен. Теперь вы можете создавать отчеты (см. стр. 588), используя этот шаблон отчета.

## Создание и просмотр отчета

► *Чтобы сформировать и просмотреть отчет:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов двойным нажатием клавиши мыши.

Отобразится выбранный шаблон отчета.

В отчете отображаются следующие данные:

- тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
- графическая диаграмма с наиболее характерными данными отчета;
- сводная таблица с вычисляемыми показателями отчета;
- таблица с детальными данными отчета.

### См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий: Мониторинг и отчеты ..... 576

## Сохранение отчета

► *Чтобы сохранить сформированный отчет:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Сохранить**.

В результате запустится мастер сохранения отчета. Следуйте далее указаниям мастера.

После завершения работы мастера откроется папка, в которую вы сохранили файл отчета.

## Создание задачи рассылки отчета

Отчеты можно рассылать по электронной почте. Рассылка отчетов в Kaspersky Security Center осуществляется с помощью задачи рассылки отчета.

► *Чтобы создать задачу рассылки одного отчета:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **Отчеты**.
3. Выберите интересующий вас шаблон отчета в списке шаблонов.
4. В контекстном меню выбранного шаблона отчета выберите пункт **Рассылка отчетов**.

В результате запускается мастер создания задачи рассылки выбранного отчета. Следуйте далее указаниям мастера.

► *Чтобы создать задачу рассылки нескольких отчетов:*

1. В дереве консоли в узле с именем нужного вам Сервера администрирования выберите папку **Задачи**.
2. В рабочей области папки **Задачи** нажмите на кнопку **Создать категорию**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

Созданная задача рассылки отчета отображается в папке дерева консоли **Задачи**.

Задача рассылки отчета создается автоматически в случае, если при установке Kaspersky Security Center были заданы параметры электронной почты (см. стр. 285).

## В этом разделе



### *Шаг 1. Выбор типа задачи*

В окне **Выбор типа задачи** в списке задач выберите тип задачи **Рассылка отчета**.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

### *Шаг 2. Выбор типа отчета*

В окне **Выбор типа отчета** в списке шаблонов для создания задачи выберите тип отчета.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

### *Шаг 3. Действия над отчетом*

В окне **Действия с отчетами** настройте следующие параметры:

- **Посылать отчеты по электронной почте**

  Если этот параметр включен, программа отправляет сформированные отчеты по электронной почте.

  Параметры отправки отчета по электронной почте можно настроить по ссылке **Параметры уведомления по электронной почте**. Ссылка доступна, когда параметр включен.

  Если этот параметр выключен, программа сохраняет отчеты в указанной папке для хранения отчетов.

  По умолчанию параметр выключен.

- **Сохранять отчеты в папке**

  Если этот параметр включен, программа сохраняет отчеты в папке, указанной в поле под флажком. Чтобы сохранять отчеты в папке общего доступа, укажите UNC-путь к этой папке. В таком случае в окне **Выбор учетной записи для запуска задачи**

необходимо задать учетную запись и пароль пользователя для доступа к этой папке.

Если этот параметр выключен, программа не сохраняет отчеты в папке, а отправляет их по электронной почте.

По умолчанию параметр выключен.

- **Замещать предыдущие отчеты того же типа**

  Если этот параметр включен, при каждом запуске задачи новый файл отчета замещает в папке для хранения отчетов файл, сохраненный при предыдущем запуске задачи.

  Если этот параметр выключен, файлы отчетов не перезаписываются. При каждом запуске задачи в папке сохраняется отдельный файл отчета.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

  По умолчанию параметр выключен.

- **Задать учетную запись для доступа к папке общего доступа**

  Если этот параметр включен, можно указать учетную запись, от имени которой отчет записывается в папку. Если в окне **Действия с отчетом** в качестве параметра **Сохранять отчет в папке** указан UNC-путь к папке общего доступа, необходимо указать учетную запись и пароль для доступа к этой папке.

  Если этот параметр выключен, отчет записывается в папку от имени учетной записи Сервера администрирования.

  Флажок доступен, если установлен флажок **Сохранять отчет в папке**.

  По умолчанию параметр выключен.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

*Шаг 4. Выбор учетной записи для запуска задачи*

В окне **Выбор учетной записи для запуска задачи** можно указать, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

- **Учетная запись по умолчанию**

  Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

  По умолчанию выбран этот вариант.

- **Задать учетную запись**

  В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль**

    Пароль учетной записи, от имени которой будет запускаться задача.

Для перехода к следующему шагу нажмите на кнопку **Далее**.

*Шаг 5. Настройка расписания задачи*

В окне **Настройка расписания запуска задачи** можно составить расписание запуска задачи. При необходимости задайте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

*Шаг 6. Определение названия задачи*

В окне **Определение названия задачи** укажите название создаваемой задачи. Имя задачи не может превышать 100 символов и не может содержать специальные символы (`"*<>?\:|`).

Для перехода к следующему шагу нажмите на кнопку **Далее**.

*Шаг 7. Завершение создания задачи*

В окне **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы завершить работу мастера.

Если вы хотите, чтобы задача запустилась сразу после завершения работы мастера создания задачи, установите флажок **Запустить задачу после завершения работы мастера**.

## Работа со статистической информацией

Статистическая информация о состоянии системы защиты и управляемых устройств отображается в виде настраиваемых информационных панелей. Статистическая информация отображается в рабочей области узла **Сервер администрирования** на закладке **Статистика**. Эта закладка также содержит несколько закладок второго уровня (страниц). На каждой странице отображаются информационные панели со статистической информацией, а также ссылки на корпоративные новости и другие материалы "Лаборатории Касперского". Статистическая информация представлена на информационных панелях в виде круговых или столбчатых диаграмм или таблиц. Данные на информационных панелях обновляются в процессе работы программы и отражают текущее состояние программы безопасности.

Можно изменить набор закладок второго уровня, содержащихся на закладке **Статистика**, набор информационных панелей на каждой странице с закладками, а также способ представления данных на информационных панелях.

► *Чтобы добавить новую закладку второго уровня с информационными панелями на закладке **Статистика**:*

1. Нажмите на кнопку **Настроить вид** в правом верхнем углу закладки **Статистика**.

   В результате откроется окно свойств статистики. В окне содержится список страниц с закладками, которые содержатся на закладке **Статистика** в настоящее время. В окне можно изменять порядок отображения страниц на закладке, добавлять и удалять страницы, переходить к настройке свойств страниц по кнопке **Свойства**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно свойств новой страницы.

3. Настройте новую страницу:

   - В разделе **Общие** укажите название страницы.
   - В разделе **Информационные панели** по кнопке **Добавить** добавьте информационные панели, которые должны отображаться на странице.

     По кнопке **Свойства** в разделе **Информационные панели** можно настраивать свойства добавленных информационных панелей: название, тип и вид диаграммы на панели, данные, по которым строится диаграмма.

4. Нажмите на кнопку **ОК**.

Добавленная страница с закладками с информационными панелями отобразится на закладке **Статистика**. Нажав на значок параметров ( ) можно сразу перейти к настройке страницы или выбранной информационной панели на странице.

## Настройка параметров уведомлений о событиях

Kaspersky Security Center позволяет выбирать способ уведомления для администратора о событиях на клиентских устройствах и настраивать параметры уведомлений.

- Электронная почта. При возникновении события программа посылает уведомление на указанные адреса электронной почты. Вы можете настроить текст уведомления.
- SMS. При возникновении события программа посылает уведомления на указанные номера телефонов. Вы можете настроить отправку SMS оповещений с помощью почтового шлюза.
- Исполняемый файл. При возникновении события на устройстве, исполняемый файл запускается на рабочем месте администратора. С помощью исполняемого файла администратор может получать параметры произошедшего события (см. стр. 321).

► *Чтобы настроить параметры уведомлений о событиях на клиентских устройствах:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно **Свойства: События**.

4. В разделе **Уведомление** выберите способ уведомления (электронная почта, SMS, исполняемый файл для запуска) и настройте параметры уведомлений:

   - **Электронная почта**

     На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес
     - Имя устройства в сети Windows (NetBIOS-имя)
     - DNS-имя SMTP-сервера

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

     Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей. По умолчанию параметр выключен.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

- Тема (название темы электронного письма).
- Адрес отправителя электронной почты.
- Параметры ESMTP-аутентификации.

  Вы должны указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

- Параметры TLS для SMTP-сервера:

  - **Не использовать TLS**

  Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

  - **Использовать TLS, если поддерживается SMTP-сервером**

  Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

  - **Всегда использовать TLS, проверить срок действия сертификата Сервера**

  Вы можете выбрать этот параметр, если хотите использовать параметры

TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы решите использовать значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать параметры TLS для SMTP-сервера:

- Выберите файл сертификата SMTP-сервера:

Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

Вы можете использовать сертификат, полученный из любого источника, например, от любого аккредитованного центра сертификации. Вы должны указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

- Сертификат X-509:

  Вы должны указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

- Контейнер с сертификатом в формате PKCS#12:

  Вы должны загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Программа отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

  На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

  В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

  В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес
  - Имя устройства в сети Windows (NetBIOS-имя)
  - DNS-имя SMTP-сервера

  В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

  Перейдите по ссылке **Параметры**, чтобы задать дополнительные параметры:

  - Тема (название темы электронного письма).
  - Адрес отправителя электронной почты.
  - Параметры ESMTP-аутентификации.

    Если необходимо, вы можете указать учетную запись для аутентификации на SMTP-сервере, если для SMTP-сервера включен параметр ESMTP-аутентификации.

  - Параметры TLS для SMTP-сервера

    Вы можете отключить использование TLS, использовать TLS, если SMTP-сервер поддерживает этот протокол, или вы можете принудительно использовать только TLS. Если вы решите использовать только TLS, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также, если вы решили использовать только TLS, вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

  - Выберите файл сертификата SMTP-сервера

    Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его в Kaspersky Security Center. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

  Вы должны загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый

ключ не зашифрован. В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив новые подстановочные параметры с подробными данными события. Список подстановочных параметров доступен по нажатию на кнопку справа от поля.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По кнопке **Отправить тестовое сообщение** проверьте, правильно ли настроены уведомления. Программа отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

  По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

1. В поле **Текст уведомления** введите текст, который программа будет отправлять при возникновении события.

   Из раскрывающегося списка, расположенного справа от текстового поля, можно добавлять в сообщение подстановочные параметры с деталями события (например, описание события, время возникновения и прочее).

   > Если текст уведомления содержит символ %, нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

2. По кнопке **Отправить пробное сообщение** проверьте, правильно ли настроены уведомления.

   Программа отправляет тестовое уведомление указанному получателю.

3. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

В результате настроенные параметры уведомления распространяются на все события, происходящие на клиентских устройствах.

Можно изменить значения параметров уведомлений для определенных событий в разделе **Настройка событий** параметров Сервера администрирования, параметров политики (см. стр. 748) или параметров программы (см. стр. 843).

См. также:

Обработка и хранение событий на Сервере администрирования ..... 686
Сценарий: Мониторинг и отчеты ..... 576

## Создание сертификата для SMTP-сервера

Сертификат для SMTP-сервера необходим для идентификации и верификации почтового сервера, к которому производится подключение. Сертификат используется для защиты пересылаемых писем от перехвата, например, в процессе передачи писем от почтового клиента к серверу и обратно.

► *Чтобы создать сертификат для SMTP-сервера:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. По ссылке **Настроить параметры уведомлений и экспорта событий** в раскрывающемся списке выберите значение **Настроить параметры уведомлений**.

   Откроется окно свойств событий.
4. На закладке **Электронная почта** по ссылке **Параметры** откройте окно **Параметры**.
5. В окне **Параметры** по ссылке **Задать сертификат** откройте окно **Сертификат для подписи**.
6. В окне **Сертификат для подписи** нажмите на кнопку **Задать**.

   В результате откроется окно **Сертификат**.
7. В раскрывающемся списке **Тип сертификата** выберите открытый или закрытый тип сертификата:
   - Если выбран сертификат закрытого типа (**Контейнер PKCS#12**), укажите файл сертификата и пароль.
   - Если выбран сертификат открытого типа (**X.509-сертификат**):
     a. укажите файл закрытого ключа (файл с расширением prk или pem);
     b. укажите пароль закрытого ключа;
     c. укажите файл открытого ключа (файл с расширением cer).
8. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для SMTP-сервера.

## Выборки событий

Информация о событиях в работе Kaspersky Security Center и управляемых программ сохраняется как в базе данных Сервера администрирования, так и в системном журнале Microsoft Windows. Вы можете просматривать информацию из базы данных Сервера администрирования в рабочей области узла **Сервер администрирования** на закладке **События**.

Информация на закладке **События** представлена в виде списка выборок событий. Каждая выборка включает в себя только события определенного типа. Например, выборка "Статус устройства – Критический" содержит только записи об изменении статусов устройств на "Критический". После установки программы на закладке **События** содержится ряд стандартных выборок событий. Вы можете создавать дополнительные (пользовательские) выборки событий, а также экспортировать информацию о событиях в файл.

kaspersky

## В этом разделе



## Просмотр выборки событий

► *Чтобы просмотреть выборку событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите нужную вам выборку событий.

   Если вы хотите, чтобы события этой выборки отображались в рабочей области постоянно, нажмите на значок "Избранное" ( ☆ ) рядом с выборкой.

В результате в рабочей области будет представлен список событий выбранного типа, хранящихся на Сервере администрирования.

Вы можете сортировать информацию в списке событий по возрастанию или убыванию данных в любой графе списка.

## Настройка параметров выборки событий

► *Чтобы настроить параметры выборки событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Откройте нужную вам выборку событий на закладке **События**.
4. Нажмите на кнопку **Свойства**.

В открывшемся окне свойств выборки событий вы можете настроить параметры выборки.

## См. также:



## Создание выборки событий

► *Чтобы создать выборку событий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.

3. Нажмите на кнопку **Создать выборку**.
4. В открывшемся окне **Новая выборка событий** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в раскрывающемся списке **Выборки событий** будет создана выборка с указанным вами именем.

По умолчанию созданная выборка событий содержит все события, хранящиеся на Сервере администрирования. Чтобы в выборке отображались только интересующие вас события, нужно настроить параметры выборки.

### См. также:

Сценарий: Мониторинг и отчеты .....576

## Экспорт выборки событий в текстовый файл

► *Чтобы экспортировать выборку событий в текстовый файл:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Нажмите на кнопку **Импорт/Экспорт**.
4. В раскрывающемся списке выберите **Экспортировать события в файл**.

В результате запустится мастер экспорта событий. Следуйте далее указаниям мастера.

### См. также:

Сценарий: Мониторинг и отчеты .....576

## Удаление событий из выборки

► *Чтобы удалить события из выборки:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. Выберите события, которые требуется удалить, с помощью мыши и клавиш **SHIFT** или **CTRL**.
4. Удалите выбранные события одним из следующих способов:
   - В контекстном меню любого из выделенных событий выберите пункт **Удалить**.

     При выборе пункта контекстного меню **Удалить все** из выборки будут удалены все отображаемые события, независимо от того, какие из них вы предварительно выбрали для удаления.
   - По ссылке **Удалить событие**, если выбрано одно событие, или по ссылке **Удалить события**, если выбрано несколько событий, в блоке работы с выбранными событиями.

В результате выбранные события будут удалены.

## Добавление программ в исключения по запросам пользователей

Если вы получаете запросы пользователей для разблокирования ошибочно заблокированных программ, вы можете создать исключение из правил Адаптивного контроля аномалий для этих программ. Такие программы больше не будут блокироваться на устройствах пользователей. Вы можете отслеживать количество запросов пользователей на закладке **Мониторинг** в рабочей области Сервера администрирования.

► *Чтобы добавить программу, заблокированную Kaspersky Endpoint Security, в исключения по запросам пользователей:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В рабочей области узла выберите закладку **События**.
3. В раскрывающемся списке **Выборки событий** выберите выборку событий **Запросы пользователей**.
4. В контекстном меню запроса пользователя (или нескольких запросов пользователей), содержащих программы, которые необходимо добавить в исключения, выберите пункт **Добавить исключения**.

   Запустится мастер добавления исключений (см. стр. 823). Следуйте шагам мастера.

Выбранные программы будут исключены из списка **Срабатывание правил в интеллектуальном режиме** (в папке **Хранилища** дерева консоли) после следующей синхронизации клиентского устройства с Сервером администрирования. Такие программы больше не будут отображаться в списке.

# Выборки устройств

Информация о состоянии устройств содержится в дереве консоли в папке **Выборки устройств**.

Информация в папке **Выборки устройств** представлена в виде списка выборок устройств. Каждая выборка включает в себя устройства, отвечающие определенным условиям. Например, выборка **Устройства со статусом "Критический"** содержит только устройства со статусом *Критический*. После установки программы папка **Выборки устройств** содержит ряд стандартных выборок. Вы можете создавать дополнительные (пользовательские) выборки устройств, экспортировать параметры выборок в файл, а также создавать выборки с параметрами, импортированными из файла.

## В этом разделе



## Просмотр выборки устройств

► *Чтобы просмотреть выборку устройств:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки в списке **Устройства выборки** выберите нужную вам выборку устройств.
3. Нажмите на кнопку **Запустить выборку**.

4. Выберите закладку **Результаты выборки**.

В результате в рабочей области отобразится список устройств, отвечающих параметрам выборки.

Вы можете сортировать информацию в списке устройств по возрастанию или убыванию данных в любой из граф.

## Настройка выборки устройств

► *Чтобы настроить параметры выборки устройств:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки перейдите на закладку **Выборка** и выберите нужную вам выборку устройств в списке пользовательских выборок устройств.
3. Нажмите на кнопку **Свойства**.
4. В открывшемся окне свойств задайте следующие параметры:
   - Общие параметры выборки.
   - Условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку. Чтобы настроить условия, выберите имя условия и нажмите на кнопку **Свойства**.
   - Параметры безопасности.
5. Нажмите на кнопку **ОК**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

**Общие**

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

**Инвертировать условие выборки**

Если этот параметр включен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию параметр выключен.

**Сеть**

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя), IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Отображаются все устройства, входящие в указанный Windows-домен.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Описание** допустимо использовать следующие символы:

  - Внутри одного слова:
    - *****. Заменяет любую строку длиной 0 и более символов.

      **Пример**:

      Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

      **Пример**:

      Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

      Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.
  - Для связи нескольких слов:
    - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

      **Пример**:

      Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

    - **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

      **Пример**:

      Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

    - **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

      **Пример**:

      Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

    - **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

      **Пример**:

      Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию параметр выключен.

### Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

  Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

  Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

  По умолчанию параметр выключен.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

### Active Directory

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию параметр выключен.

- **Устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

### Сетевая активность

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Это устройство является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут включены устройства, являющиеся точками распространения.
- **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- **Устройство в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. Программа включает в выборку устройства, которые видимы в сети в

настоящий момент.

- **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано**. Критерий не применяется.

**Программа**

В разделе **Программа** можно настроить критерии включения устройств в выборку на основании выбранной управляемой программы:

- **Имя программы**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

  В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

  Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Программа безопасности установлена**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

- **Да**. Программа включает в выборку устройства, на которых установлена программа безопасности.
- **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
- **Значение не выбрано**. Критерий не применяется.

**Операционная система**

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы:

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Разрядность операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

**Статус устройства**

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемой программы:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический* или *Предупреждение*.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК*, *Критический* или *Предупреждение*.

- **Статус постоянной защиты:**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

**Компоненты защиты**

В разделе **Компоненты защиты** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

  По умолчанию параметр выключен.

- **Всего обнаружено угроз**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

**Реестр программ**

В разделе **Реестр программ** можно настроить критерии включения устройств в выборку в зависимости от того, какие программы на них установлены:

- **Имя программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки флажка названия полей ввода **Название программы**, **Версия программы** и **Статус программы** меняются на **Имя обновления**, **Версия обновления** и **Статус** соответственно.

  По умолчанию параметр выключен.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

  В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применять к устройствам без выбранных тегов**

Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

  Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

**Реестр оборудования**

В разделе **Оборудование** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

  Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

  Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

**Виртуальные машины**

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

- **Неважно**.
- **Нет**. Искомые устройства не должны являться виртуальными машинами.
- **Да**. Искомые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да** или **Неважно**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Неважно**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

**Уязвимости и обновления**

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

**WUA переключен на Сервер администрирования**

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

**Пользователи**

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

**Проблемы, связанные со статусом управляемых программ**

В разделе **Проблемы, связанные со статусом управляемых программ** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемой программой. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких программ, у вас есть возможность автоматически выбрать эту проблему во всех списках.

**Описание статуса устройства**

Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

**Статусы компонентов управляемых программ**

В разделе **Статусы компонентов управляемых программ** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу защиты данных от утечек (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, Сбой).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

**Шифрование**

**Алгоритм шифрования**

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56*, *AES128*, *AES192* и *AES256*.

**Облачные сегменты**

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать сегмент поиска.

  Если также включен параметр **Включать дочерние объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

  В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

- **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.
- **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.
- **Google Cloud.** Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google.
- **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но недоступно для поиска с помощью API.
- **Не задано**. Условие не применяется.

**Компоненты программы**

Этот раздел содержит список компонентов тех программ, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

В разделе **Компоненты программы** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранной программе:

- **Статус**

Поиск устройств в соответствии со статусом компонента, отправленным управляемой программой на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства*, *Остановлено*, *Запускается*, *Приостановлено*, *Выполняется*, *Сбой* или *Не установлено*. Если выбранный компонент программы, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные программами:

- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемой программе.
- *Сбой* – во время выполнения операции компонента произошла ошибка.
- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки программы.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемой программой. Этот параметр показывает, что программы не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одной из программ, установленных на устройстве, или устройство выключено.

- **Версия**

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

## Экспорт параметров выборки устройств в файл

► *Чтобы экспортировать параметры выборки устройств в текстовый файл:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки на закладке **Выборки** выберите нужную вам выборку устройств в списке пользовательских выборок устройств.

   Параметры можно экспортировать только из выборок устройств, созданных пользователем.

3. Нажмите на кнопку **Запустить выборку**.
4. На закладке **Результаты выборки** нажмите на кнопку **Настройки экспорта**.
5. В открывшемся окне **Сохранить как** задайте имя файла для экспорта параметров выборки, укажите папку, в которую будет сохранен файл, и нажмите на кнопку **Сохранить**.

Параметры выборки устройств будут сохранены в указанный файл.

## Создание выборки устройств

► *Чтобы создать выборку устройств:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Создать выборку**.
3. В открывшемся окне **Новая выборка устройств** укажите имя создаваемой выборки и нажмите на кнопку **ОК**.

В результате в дереве консоли в папке **Выборки устройств** будет создана новая папка с указанным вами именем. По умолчанию созданная выборка устройств содержит все устройства, входящие в группы администрирования того Сервера, под управлением которого создана выборка. Чтобы в выборке отображались только интересующие вас устройства, нужно настроить параметры выборки по кнопке **Свойства выборки**.

## Создание выборки устройств по импортированным параметрам

► *Чтобы создать выборку устройств по импортированным параметрам:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. В рабочей области папки нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите **Импортировать**.
3. В открывшемся окне укажите путь к файлу, из которого вы хотите импортировать параметры выборки. Нажмите на кнопку **Открыть**.

В результате в папке **Выборки устройств** будет создана выборка **Новая выборка**. Параметры новой выборки параметры импортированы из указанного файла.

Если в папке **Выборки устройств** уже существует выборка с названием **Новая выборка**, к имени созданной выборки добавится окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

### Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► *Чтобы удалить устройства из групп администрирования:*

1. В дереве консоли выберите папку **Выборки устройств**.
2. Выберите устройства, которые требуется удалить, с помощью клавиш **Shift** или **Ctrl**.
3. Удалите выбранные устройства из групп администрирования одним из следующих способов:
   - В контекстном меню любого из выделенных устройств выберите пункт **Удалить**.
   - Нажмите на кнопку **Выполнить действие** и в раскрывающемся списке выберите **Удалить из группы**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

## Мониторинг установки и удаления программ

Вы можете контролировать установку и удаление определенных программ на управляемых устройствах, например, определенного браузера. Чтобы использовать эту функцию, вы можете добавить программы из реестра программ в список наблюдаемых программ. При установке или удалении контролируемой программы Агент администрирования публикует соответствующие события (см. стр. 648): **Установлена наблюдаемая программа** или **Удалена наблюдаемая программа**. Вы можете контролировать эти события, используя, например, выборки событий (на стр. 600) или отчеты (на стр. 583).

Вы можете контролировать эти события, только если они хранятся в базе данных Сервера администрирования.

► *Чтобы добавить программу в список наблюдаемых программ:*

1. В дереве консоли в папке **Дополнительно** → **Управление программами** выберите вложенную папку **Реестр программ**.
2. Над списком программ, который отображается, нажмите на кнопку **Открыть окно свойств реестра программ**.
3. В открывшемся окне **Наблюдаемые программы** нажмите на кнопку **Добавить**.
4. В открывшемся окне **Выберите название программы** выберите программу из реестра программы, установку или удаление которых вы хотите контролировать.
5. В окне **Выберите название программы** нажмите на кнопку **ОК**.

После того, как вы настроили список наблюдаемых программ и установили или удалили наблюдаемую программу на устройствах в вашей организации, вы можете контролировать соответствующие события, например, с помощью выборки событий Последние события.

# События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования, Сервере iOS MDM и Сервере мобильных устройств Exchange ActiveSync. Типы событий, которые возникают в программах "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

## В этом разделе



## Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Kaspersky Security Center, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

  Можно изменить время хранения событий:

  - Консоль администрирования: Настройка срока хранения события (см. стр. 686)
  - Kaspersky Security Center 14.2 Web Console: Настройка срока хранения события (см. стр. 1394)

Другие данные могут включать следующие поля:

- **event_id**: уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id**: идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity**: один из следующих уровней важности (в порядке возрастания важности):

  0) Недопустимый уровень важности.

  1) Информационное.

  2) Предупреждение.

  3) Ошибка.

  4) Критическое.

## События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

### В этом разделе



### Критические события Сервера администрирования

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Критическое событие**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 59. Критические события Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Лицензионное ограничение превышено.** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения.<br>События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц (на стр. 343), охватываемых лицензией.<br>Даже если возникает это событие, клиентские устройства защищены.<br>Вы можете ответить на событие следующими способами:<br>• Просмотрите список управляемых устройств. Удалите устройства, которые не используются.<br>• Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования).<br>Kaspersky Security Center определяет правила генерации событий (на стр. 341) при превышении лицензионного ограничения. | 180 дней |
| **Вирусная атака.** | 26 (для компонента Защита от файловых угроз) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (на стр. 687).<br>• Создайте более строгую политику (на стр. 432), которая будет активирована, или создайте задачу (на стр. 413), которая будет запускаться при возникновении этого события. | |
| **Вирусная атака.** | 27 (для компонента Защита от почтовых угроз) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (на стр. 687).<br>• Создайте более строгую политику (на стр. 432), которая будет активирована, или создайте задачу (на стр. 413), которая будет запускаться при возникновении этого события. | 180 дней |
| **Вирусная атака.** | 28 (для сетевого экрана) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (на стр. 687).<br>• Создайте более строгую политику (на стр. 432), которая будет | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | активирована, или создайте задачу (на стр. 413), которая будет запускаться при возникновении этого события. | |
| **Устройство стало неуправляемым.** | 4111 | KLSRV_HOST_OUT_CONTROL | События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода.<br>Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства. | 180 дней |
| **Статус устройства "Критический".** | 4113 | KLSRV_HOST_STATUS_CRITICAL | События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия (на стр. 727) при выполнении которых, статус устройства изменяется на *Критический*. | 180 дней |
| **Файл ключа в списке запрещенных.** | 4124 | KLSRV_LICENSE_BLACKLISTED | События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список.<br>Обратитесь в Службу технической поддержки (см. стр. 1489) для получения подробной информации. | 180 дней |
| **Режим ограниченной функциональности.** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | События этого типа возникают, если Kaspersky Security Center начинает работать в режиме базовой функциональности (на стр. 356), без поддержки Управления мобильными устройствами и Системного администрирования.<br>Ниже приведены причины и соответствующие ответы на событие:<br>• Срок действия лицензии истек. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Предоставьте лицензию на полную функциональность Kaspersky Security Center (добавьте действительный код активации или файл ключа на Сервер администрирования).<br>• Сервер администрирования управляет большим количеством устройств, чем может использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено). | |
| **Срок действия лицензии истекает.** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии (на стр. 342).<br>Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня.<br>После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (на стр. 356).<br>Вы можете ответить на событие | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | следующими способами:<br>• Убедитесь, что резервный лицензионный ключ (на стр. 344) добавлен на Сервер администрирования.<br>• Если вы используете подписку (на стр. 345), продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена. | |
| **Срок действия сертификата истек.** | 4132 | KLSRV_CERTIFICATE_EXPIRED | События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для Управления мобильными устройствами.<br>Вам необходимо обновить сертификат, срок действия которого истекает.<br>Вы можете настроить автоматическое обновление сертификатов, установив флажок **Автоматически перевыпускать сертификат, если это возможно** в параметрах выпуска сертификата. | 180 дней |
| **Обновления модулей программ "Лаборатории Касперского" отозваны.** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | События этого типа возникают, если обновления (на стр. 1259)были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус*Отозвано*. Событие не относится к патчам Kaspersky Security Center и не относится к модулям управляемых программ "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены. | 180 дней |

kaspersky

## См. также:



## События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 60. События отказа функционирования Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Ошибка времени выполнения.** | 4125 | KLSRV_RUNTIME_ERROR | События этого типа возникают из-за неизвестных проблем.<br>Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением.<br>Подробную информацию о событии можно найти в его описании. | 180 дней |
| **Для одной из групп лицензионных программ превышено ограничение числа установок.** | 4126 | KLSRV_INVLICPROD_EXCEDED | Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | лицензионными ключами программ сторонних производителей и если количество установок превысило заданное в лицензионном ключе программы стороннего производителя ограничение.<br>Вы можете ответить на событие следующими способами:<br>• Просмотрите список управляемых устройств. Удалите программу стороннего производителя с устройств, на которых она не используется.<br>• Используйте лицензию стороннего производителя на большее количество устройств.<br>Вы можете управлять лицензионными ключами программ сторонних производителей (на стр. 573), используя функциональность групп лицензионных программ. В группу лицензионных программ входят программы сторонних производителей, отвечающие заданным вами критериям. | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Не удалось выполнить опрос облачного сегмента.** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом. | Не хранится |
| **Не удалось выполнить копирование обновлений в заданную папку.** | 4123 | KLSRV_UPD_REPL_FAIL | События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки).<br>Вы можете ответить на событие следующими способами:<br>• Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись.<br>• Проверьте, не были ли изменены имя пользователя и / или пароль к папке (к папкам).<br>• Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и программных | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | модулей (на стр. 461). | |
| **Нет свободного места на диске.** | 4107 | KLSRV_DISK_FULL | События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство.<br>Освободите дисковое пространство на устройстве. | 180 дней |
| **Недоступна папка общего доступа.** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | События этого типа возникают, если общая папка Сервера администрирования (на стр. 236)недоступна.<br>Вы можете ответить на событие следующими способами:<br>• Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен.<br>• Проверьте, были ли изменены имя пользователя и / или пароль к папке.<br>• Проверьте подключение к сети. | 180 дней |
| **Недоступна база данных Сервера администрирования.** | 4109 | KLSRV_DATABASE_UNAVAILABLE | События этого типа возникают, если база Сервера администрирования становится недоступной.<br>Вы можете ответить на событие следующими способами: | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер.<br>• Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен. | |
| **Нет свободного места в базе данных Сервера администрирования.** | 4110 | KLSRV_DATABASE_FULL | События этого типа возникают, если нет свободного места в базе Сервера администрирования.<br>Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна.<br>Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие:<br>• Вы используете SQL Server Express Edition:<br>Проверьте в | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.<br>• Вы используете СУБД, отличную от SQL Server Express Edition:<br>Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>Сократите список событий для хранения в базе данных Сервера администрирования (на | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | стр. 1394). Просмотрите информацию о выборе СУБД (на стр. 164). | |

## См. также:



## События предупреждения Сервера администрирования

В следующей таблице приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 61. События предупреждения Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Обнаружено получение частого события.** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | События этого типа возникают, если Сервер администрирования регистрирует частые события на устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий (см. стр. 651). | 90 дней |
| **Лицензионное ограничение превышено.** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц (на стр. 343) одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией.<br>Даже если возникает это событие, клиентские устройства защищены.<br>Вы можете ответить на событие следующими способами:<br>• Просмотрите список управляемых устройств. Удалите устройства, которые не используются.<br>• Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования).<br>Kaspersky Security Center определяет правила генерации событий (на стр. 341) при превышении лицензионного ограничения. | |
| **Устройство долго не проявляет активности в сети.** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени.<br>Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации.<br>Вы можете ответить на событие следующими способами: | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Удалите устройство из списка управляемых устройств вручную.<br>• Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Консоли администрирования (см. стр. 656) или с помощью Kaspersky Security Center 14.2 Web Console (см. стр. 1131).<br>• Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования (на стр. 656) или Kaspersky Security Center 14.2 Web Console (на стр. 1131). | |
| **Конфликт имен устройств.** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство.<br>Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания программ на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве.<br>Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска (на стр. 867) на эталонном устройстве. | 90 дней |
| **Статус устройства** | 4114 | KLSRV_HOST_STATUS_WARNING | События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **"Предупреждение".** | | | Вы можете настроить условия (на стр. 727) при выполнении которых, статус устройства изменяется на *Предупреждение*. | |
| **Для одной из групп лицензионных программ скоро будет превышено ограничение числа установок.** | 4127 | KLSRV_INVLICPROD_FILLED | События этого типа возникают, если количество установок программ сторонних производителей, включенных в группу лицензионных программ (на стр. 554), достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа (на стр. 573).<br>Вы можете ответить на событие следующими способами:<br>• Если программа стороннего производителя не используется на каких-то управляемых устройствах, удалите программу с этих устройств.<br>• Если вы ожидаете, что количество установок для программы стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии программы стороннего производителя на большее количество устройств заранее.<br>Вы можете управлять лицензионными ключами программ сторонних производителей (на стр. 573), используя функциональность групп лицензионных программ. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Сертификат запрошен.** | 4133 | KLSRV_CERTIFICATE_REQUESTED | События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами.<br>Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие:<br>• Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно** выключен. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную.<br>• Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи. | 90 дней |
| **Сертификат удален.** | 4134 | KLSRV_CERTIFICATE_REMOVED | События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами.<br>После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования.<br>Это событие может быть полезно при исследовании неисправностей, | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | связанных с Управлением мобильными устройствами. | |
| **Срок действия APNs-сертификата истек.** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | События этого типа происходят, если истекает срок действия APNs-сертификата.<br>Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. | Не хранится |
| **Срок действия APNs-сертификата истекает.** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней.<br>При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM.<br>Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия. | Не хранится |
| **Не удалось отправить GCM-сообщение на мобильное устройство.** | 4138 | KLSRV_GCM_DEVICE_ERROR | События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes"). | |
| **HTTP ошибка при отправке GCM сообщения на GCM сервер.** | 4139 | KLSRV_GCM_HTTP_ERROR | События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK).<br>Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие:<br>• Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes").<br>• Проблемы на стороне прокси-сервера (если вы используете | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом. | |
| **Не удалось отправить GCM-сообщение на GCM сервер.** | 4140 | KLSRV_GCM_GENERAL_ERROR | События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging.<br>Прочтите информацию в описании события и отреагируйте соответствующим образом.<br>Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского". | 90 дней |
| **Мало свободного места на диске.** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство.<br>Освободите дисковое пространство на устройстве. | 90 дней |
| **Мало свободного места в информационной базе Сервера администрирования.** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие.<br>Вы используете SQL Server Express Edition:<br>• Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных.<br>• Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.<br>Вы используете СУБД, отличную от SQL Server Express Edition:<br>• Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394). | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Просмотрите информацию о выборе СУБД (на стр. 164). | |
| **Разорвано соединение с подчиненным Сервером администрирования.** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования.<br>Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом. | 90 дней |
| **Разорвано соединение с главным Сервером администрирования.** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | События этого типа возникают при разрыве соединения с главным Сервером администрирования.<br>Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом. | 90 дней |
| **Зарегистрированы новые обновления модулей программ "Лаборатории Касперского".** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | События этого типа возникают, если Сервер администрирования регистрирует новые обновления программ "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение.<br>Одобрите или отклоните обновления с помощью Консоли администрирования (на стр. 493) или Kaspersky Security Center Web Console (на стр. 1259). | 90 дней |
| **Началось удаление событий из базы данных, так как превышено** | 4145 | KLSRV_EVP_DB_TRUNCATING | События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в | Не хранится |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **ограничение числа событий.** | | | базе данных Сервера администрирования (на стр. 686).<br>Вы можете ответить на событие следующими способами:<br>• Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394). | |
| **Удалены события из базы данных, так как превышено ограничение числа событий.** | 4146 | KLSRV_EVP_DB_TRUNCATED | События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (на стр. 686).<br>Вы можете ответить на событие следующими способами:<br>• Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394). | Не хранится |

## См. также:

## Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

*Таблица 62. Информационные события Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Ключ использован более чем на 90%.** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | 30 дней | |
| **Найдено новое устройство.** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | 30 дней | |
| **Устройство автоматически добавлено в группу.** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 дней | |
| **Устройство удалено из группы: долгое отсутствие активности в сети.** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | 30 дней | |
| **Для одной из групп лицензионных программ число разрешенных установок исчерпано более чем на 95%.** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | 30 дней | |
| **Появились файлы для отправки на анализ в "Лабораторию Касперского".** | 4131 | KLSRV_APS_FILE_APPEARED | 30 дней | |
| **Регистрационный GCM-идентификатор мобильного устройства изменен.** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | 30 дней | |
| **Обновления успешно скопированы в заданную папку.** | 4122 | KLSRV_UPD_REPL_OK | 30 дней | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Установлено соединение с подчиненным Сервером администрирования.** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 30 дней | |
| **Установлено соединение с главным Сервером администрирования.** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | 30 дней | |
| **Базы обновлены.** | 4144 | KLSRV_UPD_BASES_UPDATED | 30 дней | |
| **Аудит: Установлено соединение с Сервером администрирования.** | 4147 | KLAUD_EV_SERVERCONNECT | 30 дней | |
| **Аудит: Изменение объекта.** | 4148 | KLAUD_EV_OBJECTMODIFY | 30 дней | Это событие отслеживает изменения в следующих объектах:<br>• группах администрирования;<br>• группах пользователей;<br>• пользователях;<br>• инсталляционных пакетах;<br>• задачах;<br>• политиках;<br>• Серверах администрирования; |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| | | | | • виртуальный Сервер. |
| **Аудит: Изменение статуса объекта.** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 30 дней | Например, это событие возникает, если задача завершилась ошибкой. |
| **Аудит: Изменение параметров группы.** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | 30 дней | |
| **Аудит: Отключено от Сервера администрирования.** | 4151 | KLAUD_EV_SERVERDISCONNECT | 30 дней | |
| **Аудит: Изменение параметров объекта.** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 дней | Это событие отслеживает изменения в следующих параметрах:<br>• Пользователь<br>• лицензия;<br>• Серверах администрирования<br>• виртуальный Сервер. |
| **Аудит: Изменение параметров разрешений.** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 30 дней | |
| **Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования.** | 5100 | KLAUD_EV_DPEKEYSEXPORT | 30 дней | |

## События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

kaspersky

## В этом разделе



## События отказа функционирования Агента администрирования

В таблице ниже приведены типы событий Агента администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 63. События отказа функционирования Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Ошибка при установке исправления.** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 476) прошла неуспешно. Событие не относится к обновлениям управляемых программ "Лаборатории Касперского".<br>Прочтите описание события. Причиной этого события может быть проблема операционной системы | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему. | |
| **Не удалось установить обновления стороннего производителя.** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами (на стр. 353), и если обновление программного обеспечения сторонних производителей (на стр. 488) прошло неуспешно.<br>Проверьте, корректна ли ссылка на программу стороннего производителя. Прочтите описание события. | 30 дней |
| **Не удалось установить обновления Центра** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | События этого типа возникают, если обновления | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **обновления Windows.** | | | Центра обновления Windows были неуспешными. Настройте обновления Microsoft Windows в политике Агента администрирования (на стр. 513).<br>Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно. | |

## См. также:



## События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Предупреждение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 64. События предупреждения Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Установка обновления программных модулей завершена с предупреждением.** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 30 дней |
| **Установка обновления стороннего ПО завершена с предупреждением.** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 30 дней |
| **Установка обновления стороннего ПО отложена.** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | 30 дней |
| **Произошел инцидент.** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 30 дней |
| **Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN.** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 30 дней |

## См. также:


События отказа функционирования Агента администрирования .....645

Информационные события Агента администрирования .....648


## Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Информационное событие**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 65. Информационные события Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Обновление программных модулей успешно установлено.** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 дней |
| **Запущена установка обновления программных модулей.** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 дней |
| **Установлена программа.** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 дней |
| **Программа удалена.** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 дней |
| **Установлена наблюдаемая программа.** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 дней |
| **Установлена наблюдаемая программа.** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 дней |
| **Установлена сторонняя программа.** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 дней |
| **Новое устройство добавлено.** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 дней |
| **Устройство удалено.** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 дней |
| **Обнаружено устройство.** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 дней |
| **Устройство авторизовано.** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 дней |
| **Совместный доступ к рабочему столу Windows: файл был прочитан.** | 7712 | KLUSRLOG_EV_FILE_READ | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Совместный доступ к рабочему столу Windows: файл был изменен.** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 дней |
| **Совместный доступ к рабочему столу Windows: программа была запущена.** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 дней |
| **Совместный доступ к рабочему столу Windows: запускается.** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 дней |
| **Совместный доступ к рабочему столу Windows: Остановлена.** | 7716 | KLUSRLOG_EV_WDS_END | 30 дней |
| **Установка обновления стороннего ПО завершена успешно.** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 дней |
| **Запущена установка обновления стороннего ПО.** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно.** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 дней |
| **Прокси-сервер KSN был остановлен.** | 7720 | KSNPROXY_STOPPED | 30 дней |

### См. также:



## Блокировка частых событий

В этом разделе представлена информация о частых событиях, блокировке отмене блокировки частых событий, экспорте списка частых событий в файл.

### В этом разделе



### О блокировке частых событий

Управляемая программа, например Kaspersky Endpoint Security для Windows, установленная на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных (на стр. 983).

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Заблокированные события можно просмотреть в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать (на стр. 652) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (на стр. 652) частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку (на стр. 652) частых событий.

### См. также:



## Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете отменить блокировку и продолжать получать частые сообщения. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

► *Чтобы управлять блокировкой частых событий:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы** и выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий**:
   - Выберите параметр **Тип события** для событий, получение которых вы хотите заблокировать.
   - Отмените выбор параметра **Тип события** для событий, которые вы хотите получать и дальше.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **ОК**.

Сервер администрирования получает частые события, для которых вы отменили выбор параметра **Тип события**, и блокирует получение частых событий, для которых вы выбрали параметр **Тип события**.

### См. также:



## Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует этот тип частых событий.

► *Чтобы отменить блокировку частых событий:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы** и выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.
4. Нажмите на кнопку **Удалить**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

### См. также:

О блокировке частых событий ..... 651

### Экспорт списка частых событий в файл

► *Чтобы экспортировать список частых событий в файл:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы** и выберите раздел **Блокировка частых событий**.
3. Нажмите на кнопку **Экспортировать в файл**.
4. В открывшемся окне **Сохранить как** укажите путь к файлу, в которых вы хотите сохранить список.
5. Нажмите на кнопку **Сохранить**.

Все записи списка частых событий экспортируются в файл.

### См. также:

О блокировке частых событий ..... 651

Управление блокировкой частых событий ..... 652

## Контроль изменения состояния виртуальных машин

Сервер администрирования хранит информацию о состоянии управляемых устройств, например, реестр оборудования и список установленных программ, параметры управляемых программ, задач и политик. Если управляемым устройством является виртуальная машина, пользователь может в любой момент восстановить ее состояние из образа виртуальной машины (snapshot), сделанного ранее. В результате информация о состоянии виртуальной машины на Сервере администрирования может стать неактуальной.

Например, администратор создал политику защиты на Сервере администрирования в 12:00, которая начала работать на виртуальной машине VM_1 в 12:01. В 12:30 пользователь виртуальной машины VM_1 изменил ее статус, восстановив ее из снимка, сделанного в 11:00. Политика защиты перестает работать на виртуальной машине. Однако на Сервере администрирования сохранится неактуальная информация о том, что политика защиты на виртуальной машине VM_1 продолжает действовать.

Kaspersky Security Center позволяет контролировать изменение состояния виртуальных машин.

После каждой синхронизации с устройством Сервер администрирования формирует уникальный идентификатор, который хранится как на устройстве, так и на Сервере администрирования. Перед началом следующей синхронизации Сервер администрирования сравнивает значения идентификаторов на обеих сторонах. Если значения идентификаторов не совпадают, Сервер администрирования считает виртуальную машину восстановленной из образа. Сервер администрирования сбрасывает действующие для этой виртуальной машины параметры политик и задач и отправляет на нее актуальные политики и список групповых задач.

## Отслеживание состояния антивирусной защиты с помощью информации в системном реестре

► *Чтобы отследить состояние антивирусной защиты на клиентском устройстве с помощью информации, записанной Агентом администрирования в системный реестр, в зависимости от операционной системы устройства:*

- На устройствах под управлением Windows:
  1. Откройте системный реестр клиентского устройства (например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**).
  2. Перейдите в раздел:
     - Для 32-разрядных систем:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState
     - Для 64-разрядных систем:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     В результате в системном реестре отобразится информация о состоянии антивирусной защиты клиентского устройства.
- На устройствах под управлением Linux:
  - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.
- На устройствах под управление macOS:
  - Информация содержится в отдельных текстовых файлах, по одному для каждого типа данных, расположенных /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Состояние антивирусной защиты соответствует значениям ключей, описанных в таблице ниже.

*Таблица 66. Ключи реестра и их возможные значения*

| Ключ (тип данных) | Значение | Описание |
|---|---|---|
| Protection_LastConnected (REG_SZ) | ДД-ММ-ГГГГ ЧЧ-ММ-СС | Дата и время (в формате UTC) последнего соединения с Сервером администрирования. |
| Protection_AdmServer (REG_SZ) | IP, DNS-имя или NetBIOS-имя | Имя Сервера администрирования, который управляет устройством. |
| Protection_NagentVersion (REG_SZ) | a.b.c.d | Номер сборки Агента администрирования, установленного на устройстве. |
| Protection_NagentFullVersion (REG_SZ) | a.b.c.d (патч1; патч2; ...; патчN) | Номер версии Агента администрирования (с патчами), установленного на устройстве. |
| Protection_HostId (REG_SZ) | Идентификатор устройства | Идентификатор устройства. |
| Protection_DynamicVM (REG_DWORD) | 0 – нет<br>1 – да | Агент администрирования установлен в динамический режим для VDI. |
| Protection_AvInstalled (REG_DWORD) | 0 – нет<br>1 – да | Программа безопасности установлена на устройстве. |
| Protection_AvRunning (REG_DWORD) | 0 – нет<br>1 – да | Постоянная защита устройства включена. |
| Protection_HasRtp (REG_DWORD) | 0 – нет<br>1 – да | Установлен компонент постоянной защиты. |
| Protection_RtpState (REG_DWORD) | Статус постоянной защиты: | |
| | 0 | Неизвестно. |
| | 1 | Выключен |
| | 2 | Приостановлена. |
| | 3 | Запускается. |
| | 4 | Включен. |
| | 5 | Включен с высоким уровнем защиты (максимальная защита). |
| | 6 | Включен с низким уровнем защиты (максимальная скорость). |

| Ключ (тип данных) | Значение | Описание |
|---|---|---|
| | 7 | Включен с параметрами по умолчанию (рекомендуемые параметры). |
| | 8 | Включен с пользовательскими параметрами. |
| | 9 | Сбой в работе. |
| `Protection_LastFscan (REG_SZ)` | ДД-ММ-ГГГГ ЧЧ-ММ-СС | Дата и время (в формате UTC) последней полной проверки. |
| `Protection_BasesDate (REG_SZ)` | ДД-ММ-ГГГГ ЧЧ-ММ-СС | Дата и время (в формате UTC) выпуска баз программы. |

## Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

► *Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:*

1. Нажмите правой клавишей мыши на название требуемой группы администрирования.
2. В контекстном меню выберите пункт **Свойства**.

   Откроется окно свойств группы администрирования.
3. В окне свойств перейдите в раздел **Устройства**.
4. При необходимости включите или выключите следующие параметры:

   - **Уведомлять администратора, если устройство неактивно больше (сут)**

     Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

     По умолчанию параметр включен.

   - **Наследовать из родительской группы**

     Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств** недоступны для изменения.

Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование параметров для дочерних групп**

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.

5. Нажмите на кнопку **ОК**.

Ваши изменения сохранены и применены.

## Выключение объявлений "Лаборатории Касперского"

В Kaspersky Security Center 14.2 Web Console раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

► *Чтобы выключить объявления, связанные с безопасностью:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно выключить объявления, связанные с безопасностью.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования в разделе **Объявления "Лаборатории Касперского"** выключите раздел **Включить отображение объявлений "Лаборатории Касперского" в Kaspersky Security Center Web Console**.
4. Нажмите на кнопку **ОК**.

Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN (см. стр. 832).

### См. также:

kaspersky

# Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory (см. стр. 426).

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.

- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;
- множество небольших изолированных офисов.

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

kaspersky

## См. также:



## В этом разделе



# Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.
- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

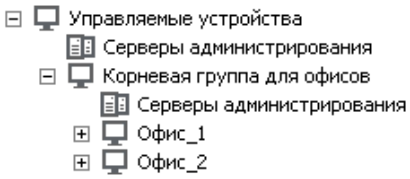
См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Типовая конфигурация точек распространения: Множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).




На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Пример: Ноутбук находится в группе администрирования **Офис 1**, но физически переехавший в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

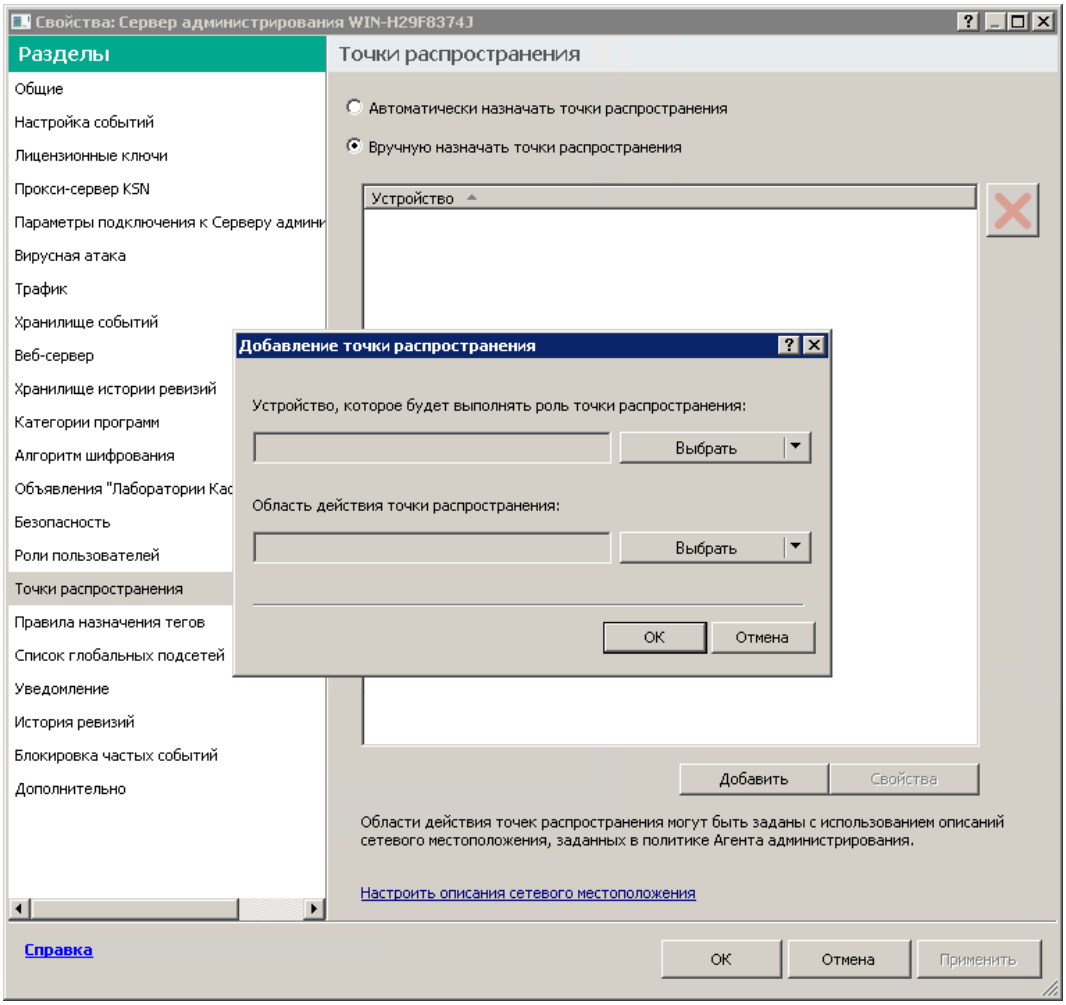
## Назначение управляемого устройства точкой распространения

Вы можете вручную назначить устройство точкой распространения для группы администрирования и настроить ее как шлюз соединений в Консоли администрирования.

► *Чтобы назначить устройство точкой распространения группы администрирования:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.
5. Нажмите на кнопку **Добавить**.




В результате откроется окно **Добавление точки распространения**.

6. В окне **Добавление точки распространения** выполните следующие действия:

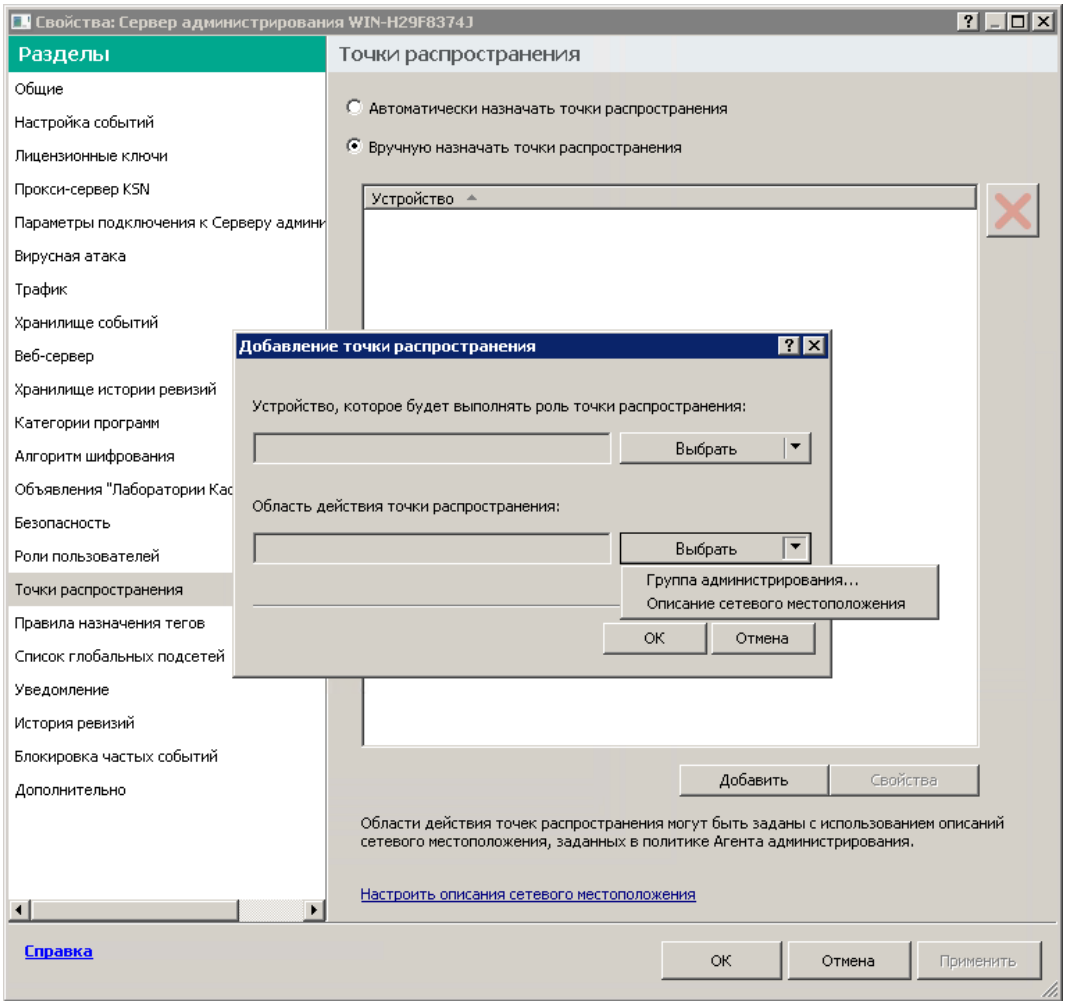
   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз рядом с кнопкой **Выбрать** и выберите вариант **Добавить устройство из группы**.

   b. В открывшемся окне **Выбрать устройства** выберите устройство, которое будет выполнять роль точки распространения.

   c. В разделе **Область действия точки распространения** нажмите на стрелку вниз (  ) рядом с разворачивающейся кнопкой **Выбрать**.

   d. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

   e. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление точки распространения**.




Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

Первое устройство с установленным Агентом администрирования, которое подключится к виртуальному Серверу администрирования, будет автоматически назначено точкой распространения и настроено в качестве шлюза соединений.

## См. также:

Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения..664

# Подключение нового сегмента сети с помощью устройств под управлением Linux

Вы можете подключить новый сегмент сети с помощью устройства под управлением Linux. Для этого нужно хотя бы два разных устройства. Одно устройство, которое можно настроить как шлюз соединения в демилитаризованной зоне, а другое устройство назначить точкой распространения.

Выполняйте процедуру, описанную в этом разделе, только после завершения основного сценария установки (на стр. 92).

► *Чтобы подключить новый сегмент сети на устройстве под управлением Linux:*

1. Подключите устройство под управлением Linux в качестве шлюза соединения в демилитаризованной зоне (на стр. 663).
2. Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения (на стр. 664).

Подключение нового сегмента сети с помощь устройства под управлением Linux настроено.

### См. также:



## Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне

► *Чтобы подключить устройство под управлением Linux в качестве шлюза в демилитаризованной зоне (DMZ):*

1. Загрузите и установите Агент администрирования на устройство Linux (на стр. 207).
2. Запустите послеустановочный скрипт и следуйте указаниям мастера, чтобы настроить конфигурацию локальной среды. В командной строке выполните следующую команду:

   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. На шаге с запросом режима Агента администрирования выберите параметр **Использовать как шлюз соединения**.
4. В открывшемся окне свойств Сервера администрирования выберите раздел **Точка распространения**.
5. В открывшемся окне **Точки распространения** в правой части окна:
   a. Выберите параметр **Вручную назначать точки распространения**.
   b. Нажмите на кнопку **Добавить**.

   В результате откроется окно **Добавление точки распространения**.
6. В окне **Добавление точки распространения** выполните следующие действия:
   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз (  ) рядом с разворачивающейся кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.
   b. В разделе **Область действия точки распространения** нажмите на стрелку вниз (  ) рядом с разворачивающейся кнопкой **Выбрать**.
   c. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования.

d. Нажмите на кнопку **ОК**, чтобы закрыть окно **Добавление точки распространения**.

7. Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.
8. Запустите утилиту klnagchk, чтобы проверить, успешно ли настроено соединение с Kaspersky Security Center. В командной строке введите команду:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

9. В главном окне программы перейдите в Kaspersky Security Center и найдите устройство (на стр. 325).
10. В появившемся окне нажмите на <Имя устройства>.
11. В раскрывающемся списке выберите ссылку **Переместить в группу**.
12. В открывшемся окне **Выбрать группу** перейдите по ссылке **Точки распространения**.
13. Нажмите на кнопку **ОК**.
14. Перезапустите службу Агента администрирования на клиенте Linux, выполнив в командной строке команду:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
```

Подключение устройства под управлением Linux в качестве шлюза в демилитаризованной зоне завершено.

## Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения

► *Чтобы подключить устройство под управлением Linux к Серверу администрирования с помощью шлюза соединения, выполните на этом устройстве следующие действия:*

1. Загрузите и установите Агент администрирования на устройство Linux (на стр. 207).
2. Запустите послеустановочный скрипт Агента администрирования, выполнив в командной строке следующую команду:

```
$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. На шаге с запросом режима Агента администрирования выберите параметр **Подключаться к Серверу через шлюз соединений** и введите адрес шлюза соединения.
4. Проверьте соединение с Kaspersky Security Center и шлюзом соединения распространения с помощью следующей команды в командной строке:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

   В выходных данных отображается адрес шлюза соединения.

Подключение устройства под управлением Linux к Серверу администрирования с помощью шлюза соединения завершено. Вы можете использовать это устройство для распространения обновлений, для удаленной установки программ и для получения информации о сетевых устройствах.

## Добавление шлюза соединения в демилитаризованной зоне в качестве точки распространения

Шлюз соединения (на стр. 90) ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования. Это означает, что сразу после установки шлюза соединения на

устройстве в демилитаризованной зоне Сервер администрирования не перечисляет устройство среди управляемых устройств. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

► *Чтобы добавить устройство со шлюзом соединения в качестве точки распространения:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
4. В правой части окна выберите параметр **Вручную назначать точки распространения**.
5. Нажмите на кнопку **Добавить**.

   В результате откроется окно **Добавление точки распространения**.
6. В окне **Добавление точки распространения** выполните следующие действия:

   a. В разделе **Устройство выполняет роль точки распространения** нажмите на стрелку вниз рядом с кнопкой **Выбрать** и выберите вариант **Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.

   b. В открывшемся окне **Ввод адреса шлюза соединений** введите IP-адрес шлюза соединения (или введите имя, если шлюз соединения доступен по имени).

   c. В разделе **Область действия точки распространения** нажмите на стрелку вниз рядом с кнопкой **Выбрать** .

   d. Укажите набор устройств, на которые точка распространения будет распространять обновления. Вы можете указать группу администрирования или описание сетевого местоположения.

      Рекомендуется создать отдельную группу для внешних управляемых устройств.

После того, как вы выполнили это действие, список точек распространения содержит новую запись с именем **Временная запись для шлюза соединений**.

Сервер администрирования практически сразу пытается подключиться к шлюзу соединения по указанному адресу. В случае успеха имя записи меняется на имя устройства шлюза соединения. Этот процесс занимает до пяти минут.

Пока временная запись для шлюза соединения преобразуется в именованную запись, шлюз соединения также появляется в группе **Нераспределенные устройства**.

### См. также:

Назначение управляемого устройства точкой распространения.....660

## Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения.

► *Чтобы назначить точки распространения автоматически:*

1. Откройте главное окно программы.

2. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется автоматически назначать точки распределения.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
5. В правой части окна выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

6. Нажмите на кнопку **ОК**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## О локальной установке Агента администрирования на устройство, выбранное точкой распространения

Чтобы устройство, выбранное точкой распространения, могло напрямую связаться с виртуальным Сервером администрирования для выполнения роли шлюза соединений, на это устройство требуется локально установить Агент администрирования.

Порядок локальной установки Агента администрирования на устройство, выбранное точкой распространения, совпадает с порядком локальной установки Агента администрирования на любое устройство сети.

Для устройства, выбранного точкой распространения, должны быть выполнены следующие условия:

- В процессе локальной установки Агента администрирования в окне мастера установки **Сервер администрирования** в поле **Адрес сервера** требуется указать адрес виртуального Сервера администрирования, под управлением которого находится устройство. В качестве адреса устройства можно использовать IP-адрес или имя устройства в сети Windows.

  Для адреса виртуального Сервера администрирования используется следующий формат: <полный адрес физического Сервера администрирования, которому подчинен виртуальный Сервер>/<Имя виртуального Сервера администрирования>.

- Для выполнения роли шлюза соединений на устройстве должны быть открыты все порты, необходимые для связи с Сервером администрирования.

В результате установки на устройство Агента администрирования с указанными параметрами программа Kaspersky Security Center автоматически выполняет следующие действия:

- включает это устройство в группу **Управляемые устройства** виртуального Сервера администрирования;
- назначает это устройство точкой распространения группы **Управляемые устройства** виртуального Сервера администрирования.

Необходимо и достаточно выполнить локальную установку Агента администрирования на устройстве, назначенном точкой распространения группы **Управляемые устройства** в сети организации. На устройства, выполняющие роль точек распространения во вложенных группах администрирования, Агент администрирования можно установить удаленно. Для этого используйте точку распространения группы **Управляемые устройства** в качестве шлюза соединений.

См. также:

Локальная установка Агента администрирования....205
Программы "Лаборатории Касперского".Централизованное развертывание....359

## Об использовании точки распространения в качестве шлюза соединений

Если Сервер администрирования находится вне демилитаризованной зоны (DMZ), Агенты администрирования, находящиеся в демилитаризованной зоне, теряют возможность соединения с ним.

Для соединения Сервера администрирования с Агентами администрирования в качестве шлюза соединений можно использовать точку распространения. Точка распространения предоставляет Серверу администрирования порт для создания соединения. В момент запуска Сервер администрирования подключается к точке распространения и не разрывает соединение с ней в течение всего времени работы.

Получив сигнал от Сервера администрирования, точка распространения посылает Агентам администрирования UDP-сигнал на подключение к Серверу администрирования. При получении сигнала Агенты администрирования подключаются к точке распространения, которая передает информацию между Агентом администрирования и Сервером администрирования. Обмен информацией может происходить по IPv4-сети или IPv6-сети.

Рекомендуется использовать в качестве шлюза соединений выделенное устройство и назначать на один шлюз соединений не более 10 000 клиентских устройств (включая мобильные устройства).

См. также:

Назначение управляемого устройства точкой распространения....660
Локальная установка Агента администрирования....205

## Добавление IP-диапазонов в список проверенных диапазонов точки распространения

Вы можете добавить IP-диапазон в список опрашиваемых диапазонов точки распространения.

► *Чтобы добавить IP-диапазон в список опрашиваемых диапазонов:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точка распространения**.

4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения выберите раздел **Обнаружение устройств** → **IP-диапазоны**.
6. Установите флажок **Разрешить опрос диапазона**.
7. Нажмите на кнопку **Добавить**.

   Кнопка **Добавить** активна, если установлен флажок **Разрешить опрос диапазона**.

   Откроется окно **IP-диапазон**.
8. В окне **IP-диапазон** введите имя нового IP-диапазона (по умолчанию указано имя Новый диапазон).
9. Нажмите на кнопку **Добавить**.
10. Выполните одно из следующих действий:
    - Задайте IP-диапазон начальным и конечным IP-адресом.
    - Задайте IP-диапазон адресом и маской подсети.
    - Нажмите на кнопку **Обзор** и добавьте подсеть из глобального списка подсетей (на стр. 934).
11. Нажмите на кнопку **ОК**.
12. Нажмите на кнопку **ОК**, чтобы добавить диапазон с заданным именем.

Новый диапазон отобразится в списке опрашиваемых диапазонов.

## Использование точки распространения в качестве извещающего сервера

В Kaspersky Security Center точка распространения может работать как push-сервер (см. стр. 668) для устройств, которые управляются по мобильному протоколу и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию (см. стр. 1272) устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемой программы или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

► *Чтобы использовать точку распространения в качестве push-сервера:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.

2. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования выберите раздел **Точка распространения**.
4. В списке выберите требуемую точку распространения и нажмите на кнопку **Свойства**.
5. В открывшемся окне свойств точки распространения в разделе **Общие** выберите параметр **Использовать точку распространения в качестве push-сервера**.
6. Укажите номер порта push-сервера, то есть того порта на точке распространения, который клиентские устройства будут использовать для подключения.

   По умолчанию номер порта – 13295.
7. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств точки распространения.
8. Откройте окно свойств политики Агента администрирования (см. стр. 750).
9. В разделе **Подключения** перейдите в подраздел **Сети**.
10. В подразделе **Сеть** выберите вариант **Использовать точку распространения для принудительного подключения к Серверу администрирования**.
11. Нажмите на кнопку **ОК**, чтобы закрыть окно.

Точка распространения начинает выполнять роль push-сервера. Теперь он может отправлять push-уведомления на клиентские устройства.

Если вы управляете устройствами с установленной операционной системой KasperskyOS или планируете это сделать, вы должны использовать точку распространения в качестве push-сервера. Вы также можете использовать точку распространения в качестве push-сервера, если хотите отправлять push-уведомления на клиентские устройства.

## См. также:


Обновление программного обеспечения на клиентском устройстве с помощью точки распространения ..... 140

Порты, используемые Kaspersky Security Center ..... 98

Точка распространения ..... 88

Настройка точек распространения и шлюзов соединений ..... 658

# Другие повседневные задачи

Этот раздел содержит рекомендации о ежедневной работе с Kaspersky Security Center.

## В этом разделе



# Управление Серверами администрирования

Этот раздел содержит информацию о работе с Серверами администрирования и о настройке параметров Сервера администрирования.

kaspersky

## В этом разделе



# Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Добавление возможно независимо от того, доступен ли Сервер, который вы хотите сделать подчиненным, для подключения через Консоль администрирования.

При объединении Серверов в иерархию необходимо, чтобы порт 13291 обоих Серверов был доступен. Порт 13291 необходим для приема подключений от Консоли администрирования к Серверу администрирования (на стр. 138).

### Подключение Сервера администрирования в качестве подчиненного к главному Серверу

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера с подключением к главному Серверу по порту 13000. Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить Сервер администрирования, доступный для подключения через Консоль, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 поддерживаемого главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Сервер администрирования** выбранной группы перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования.
6. Следуйте далее указаниям мастера.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Подчиненный Сервер будет принимать подключение от главного Сервера (на стр. 141).

Если у вас нет устройства с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования (например, если будущий подчиненный Сервер находится в удаленном офисе, а системный администратор удаленного офиса из соображений безопасности не делает доступным порт 13291 через интернет), вы все равно можете добавить подчиненный Сервер.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Консоль, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для подключения от подчиненных Серверов администрирования.
2. Запишите файл сертификата будущего главного Сервера администрирования на внешнее устройство (например, съемный диск) либо перешлите системному администратору того удаленного офиса, в котором находится Сервер администрирования.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.
3. Запишите файл сертификата будущего подчиненного Сервера администрирования на внешнее устройство (например, съемный диск). Если будущий подчиненный Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса переслать вам сертификат.

   Файл сертификата Сервера администрирования находится на Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.
4. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
5. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
6. Нажмите на кнопку **Добавить подчиненный Сервер администрирования** в рабочей области узла **Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
7. На первом шаге мастера (ввод адреса) оставьте поле **Адрес** пустым.

8. В окне **Выбор файла сертификата подчиненного Сервера администрирования** нажмите на кнопку **Обзор** и выберите сохраненный ранее файл сертификата подчиненного Сервера.
9. После завершения работы мастера подключитесь с помощью другой Консоли администрирования к будущему подчиненному Серверу администрирования. Если этот Сервер находится в удаленном офисе, попросите системного администратора удаленного офиса подключиться к будущему подчиненному Серверу администрирования и выполнить на нем дальнейшие шаги.
10. В контекстном меню узла **Сервер администрирования** выберите **Свойства**.
11. В свойствах Сервера администрирования перейдите в раздел **Дополнительно** и затем в раздел **Иерархия Серверов администрирования**.
12. Установите флажок **Данный Сервер администрирования является подчиненным в иерархии**.

    Поля ввода станут доступными для ввода и редактирования.
13. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.
14. Выберите ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.
15. Нажмите на кнопку **ОК**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Вы сможете подключаться к подчиненному Серверу через Консоль администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера (на стр. 141).

**Подключение главного Сервера администрирования к подчиненному Серверу**

Вы можете добавить новый Сервер администрирования в качестве подчиненного Сервера так, чтобы главный Сервер подключался к подчиненному Серверу по порту 13000. Это целесообразно, например, если вы размещаете подчиненный Сервер в демилитаризованной зоне.

Вам потребуется устройство с установленной Консолью администрирования, с которого доступны порты TCP 13291 обоих Серверов администрирования:

► *Чтобы добавить новый Сервер администрирования в качестве подчиненного и подключить главный Сервер к нему по порту 13000:*

1. Убедитесь, что порт 13000 будущего подчиненного Сервера доступен для приема подключений от главного Сервера администрирования.
2. С помощью Консоли администрирования подключитесь к будущему главному Серверу администрирования.
3. Выберите группу администрирования, в которую вы планируете добавить подчиненный Сервер администрирования.
4. В рабочей области узла **Сервер администрирования** нужной группы администрирования перейдите по ссылке **Добавить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
5. На первом шаге мастера (ввод адреса Сервера администрирования, добавляемого в группу) введите сетевое имя будущего подчиненного Сервера администрирования, и установите флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
6. Если вы подключаетесь к будущему подчиненному Серверу через прокси-сервер, на первом шаге мастера установите флажок **Использовать прокси-сервер** и введите параметры подключения.
7. Следуйте далее указаниям мастера.

Будет установлена иерархия Серверов администрирования. Подчиненный Сервер будет принимать подключение от главного Сервера (на стр. 142).

См. также:

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне .142

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования .....141

Порты, используемые Kaspersky Security Center.....98

## Подключение к Серверу администрирования и переключение между Серверами администрирования

При запуске программа Kaspersky Security Center предпринимает попытку соединения с Сервером администрирования. Если в сети существует несколько Серверов администрирования, запрашивается тот Сервер, с которым было установлено соединение во время предыдущего сеанса работы программы Kaspersky Security Center.

Если программа запускается в первый раз после установки, выполняется попытка соединения с Сервером администрирования, указанным при установке Kaspersky Security Center.

После соединения с Сервером администрирования структура папок этого Сервера отображается в дереве консоли.

Если в дерево консоли добавлено несколько Серверов администрирования, вы можете переключаться между ними.

Для работы с каждым Сервером администрирования необходима Консоль администрирования. Перед первым подключением к новому Серверу администрирования убедитесь, что на нем открыт порт 13291, по которому принимаются подключения от Консоли (на стр. 138), и все остальные порты для связи Сервера администрирования с другими компонентами Kaspersky Security Center (на стр. 98).

► *Чтобы переключиться на другой Сервер администрирования:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню узла выберите пункт **Подключиться к Серверу администрирования**.
3. В открывшемся окне **Параметры подключения** в поле **Адрес Сервера администрирования** укажите имя Сервера администрирования, к которому вы хотите подключиться. В качестве имени Сервера администрирования вы можете указать IP-адрес или имя устройства в сети Windows. При нажатии на кнопку **Дополнительно** в нижней части окна вы можете настроить параметры подключения к Серверу администрирования (см. рис. ниже).

   Для подключения к Серверу администрирования через порт, отличный от установленного по умолчанию, в поле **Адрес Сервера администрирования** требуется ввести значение в формате <Имя Сервера администрирования>:<Порт>.

Пользователям, не обладающим правами на **Чтение**, будет отказано в доступе к Серверу администрирования.

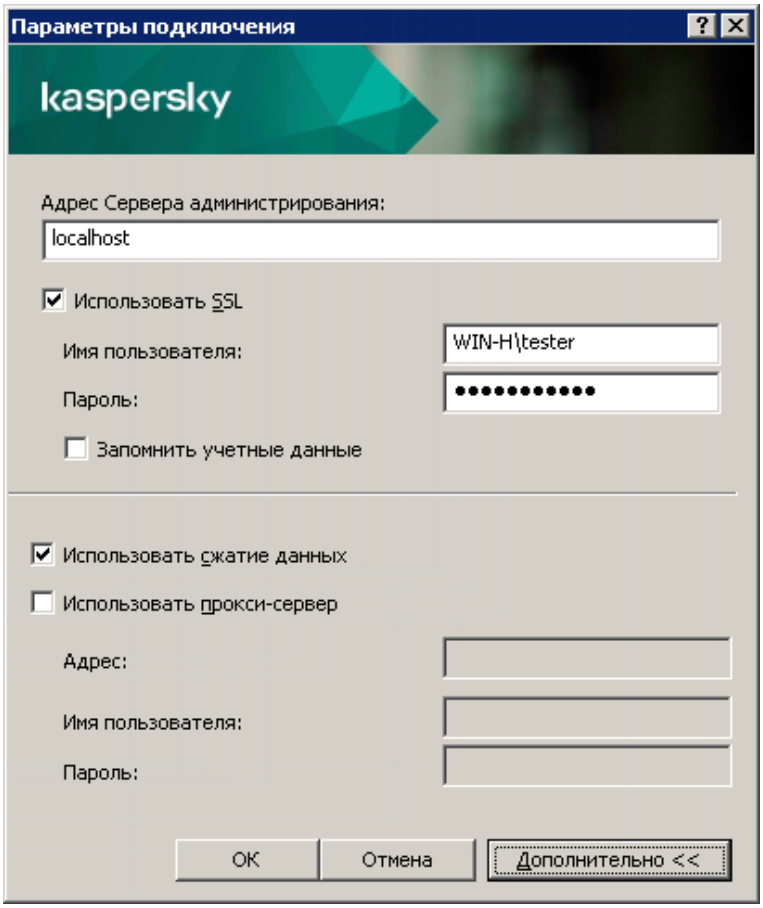



Figure 1. Установка соединения с Сервером администрирования

4. Нажмите на кнопку **ОК** для завершения переключения между Серверами.

После соединения с Сервером администрирования структура папок соответствующего ему узла в дереве консоли обновляется.

## См. также:

Порты, используемые Kaspersky Security Center ..... 98

Сервер администрирования и Консоль администрирования ..... 138

## Права доступа к Серверу администрирования и его объектам

При установке Kaspersky Security Center автоматически формируются группы пользователей **KLAdmins** и **KLOperators**. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы **KLAdmins** и **KLOperators** создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются в домене, в который входит Сервер администрирования, и на Сервере администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на Сервере администрирования.

Просмотр групп **KLAdmins** и **KLOperators** и внесение необходимых изменений в права пользователей групп **KLAdmins** и **KLOperators** можно осуществлять при помощи стандартных средств администрирования операционной системы.

Группе **KLAdmins** предоставлены все права, группе **KLOperators** – права на чтение и выполнение. Набор прав, предоставленных группе **KLAdmins**, недоступен для изменения.

Пользователи, входящие в группу **KLAdmins**, называются *администраторами Kaspersky Security Center*, пользователи из группы **KLOperators** – *операторами Kaspersky Security Center*.

Помимо пользователей, входящих в группу **KLAdmins**, права администратора Kaspersky Security Center предоставляются локальным администраторам устройств, на которых установлен Сервер администрирования.

Локальных администраторов можно исключать из списка пользователей, имеющих права администратора Kaspersky Security Center.

Все операции, запущенные администраторами Kaspersky Security Center, выполняются с правами учетной записи Сервера администрирования.

Для каждого Сервера администрирования в сети можно сформировать свою группу **KLAdmins**, обладающую правами только в рамках работы с этим Сервером.

Если устройства, относящиеся к одному домену, входят в группы администрирования разных Серверов, то администратор домена является администратором Kaspersky Security Center в рамках всех этих групп администрирования. Группа **KLAdmins** для этих групп администрирования едина и создается при установке первого Сервера администрирования. Операции, запущенные администратором Kaspersky Security Center, выполняются с правами учетной записи того Сервера администрирования, для которого они запущены.

После установки программы администратор Kaspersky Security Center может выполнять следующие действия:

- изменять права, предоставляемые группам **KLOperators**;
- определять права доступа к функциям программы Kaspersky Security Center другим группам пользователей и отдельным пользователям, зарегистрированным на рабочем месте администратора;
- определять права доступа пользователей к работе в каждой группе администрирования.

Администратор Kaspersky Security Center может назначать права доступа к каждой группе администрирования или к другим объектам Сервера администрирования в разделе **Безопасность** окна свойств выбранного объекта.

Вы можете отследить действия пользователя при помощи записей о событиях в работе Сервера администрирования. Записи о событиях отображаются в узле **Сервер администрирования** на закладке **События**. Эти события имеют уровень важности **Информационное сообщение**; типы событий начинаются со слова **Аудит**.

### См. также:

Изменения в системе после установки Kaspersky Security Center ..... 277

## Условия подключения к Серверу администрирования через интернет

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

## Защищенное подключение к Серверу администрирования

Обмен информацией между клиентскими устройствами и Сервером администрирования, а также подключение Консоли администрирования к Серверу администрирования могут производиться с использованием протокола TLS (Transport Layer Security). Протокол TLS позволяет идентифицировать стороны, взаимодействующие при подключении, осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче. В основе протокола TLS лежит аутентификация взаимодействующих сторон и шифрование данных по методу открытых ключей.

### В этом разделе

Аутентификация Сервера при подключении устройства ..... 678

Аутентификация Сервера при подключении Консоли администрирования ..... 678

kaspersky

## Аутентификация Сервера при подключении устройства

При первом подключении клиентского устройства к Серверу администрирования Агент администрирования на устройстве получает копию сертификата Сервера администрирования и сохраняет его локально.

При локальной установке Агента администрирования на устройство сертификат Сервера администрирования можно выбрать вручную.

На основании полученной копии сертификата осуществляется проверка прав и полномочий Сервера администрирования при следующих соединениях.

В дальнейшем, при каждом подключении устройства к Серверу администрирования Агент администрирования запрашивает сертификат Сервера администрирования и сравнивает его с локальной копией. Если они не совпадают, доступ Сервера администрирования к устройству не разрешается.

## Аутентификация Сервера при подключении Консоли администрирования

При первом подключении к Серверу администрирования Консоль администрирования запрашивает сертификат Сервера администрирования и сохраняет его копию локально на рабочем месте администратора. На основании полученной копии сертификата при последующих подключениях Консоли администрирования к этому Серверу администрирования осуществляется идентификация Сервера администрирования.

Если сертификат Сервера администрирования не совпадает с копией сертификата, хранящейся на рабочем месте администратора, Консоль администрирования выводит запрос на подтверждение подключения к Серверу администрирования с заданным именем и на получение нового сертификата. После подключения Консоль администрирования сохраняет копию нового сертификата Сервера администрирования, которая будет использоваться для идентификации Сервера в дальнейшем.

# Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором они могут открыть Kaspersky Security Center 14.2 Web Console или на котором установлена Консоль администрирования на основе консоли Microsoft Management Console (MMC). Настроить Сервер администрирования можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, даже если злоумышленник похитит учетную запись Kaspersky Security Center, он не сможет войти в Kaspersky Security Center, так как IP-адрес устройства злоумышленника отсутствует в списке разрешенных.

IP-адрес проверяется, когда пользователь входит в Kaspersky Security Center или запускает программу, которая взаимодействует с Сервером администрирования через Kaspersky Security Center OpenAPI (см. стр 1482). В этот момент устройство пользователя пытается установить соединение с Сервером администрирования. Если IP-адрес устройства отсутствует в списке разрешенных, возникает ошибка аутентификации и событие KLAUD_EV_SERVERCONNECT (см. стр. 1427) уведомляет о том, что соединение с Сервером администрирования не установлено.

### Требования к списку разрешенных IP-адресов

IP-адреса проверяются только при попытке подключения к Серверу администрирования следующих программ:

- Сервер Kaspersky Security Center Web Console

  Если вы входите в Web Console на одном устройстве, а Сервер Web Console установлен на другом устройстве (см. стр. 945), вы можете настроить сетевой экран на устройстве с Сервером Web Console штатными средствами операционной системы. Тогда, если кто-то попытается войти в Web Console, сетевой экран поможет предотвратить вмешательство злоумышленников.

- Консоль администрирования
- Программы, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut.
- Программы, взаимодействующие с Сервером администрирования через OpenAPI, такие как Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред.

Поэтому укажите адреса устройств, на которых установлены перечисленные выше программы.

Вы можете установить IPv4-адреса и IPv6-адреса. Указать диапазоны IP-адресов нельзя.

**Как создать список разрешенных IP-адресов**

Если вы еще не установили список разрешенных, следуйте приведенным ниже инструкциям.

► *Чтобы создать список разрешенных IP-адресов для входа в Kaspersky Security Center:*

1. На устройстве Сервера администрирования запустите командную строку под учетной записью с правами администратора.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Введите следующую команду, используя права администратора:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"<IP addresses>" -t s
```

   Укажите IP-адреса, соответствующие перечисленным выше требованиям. Несколько IP-адресов должны быть разделены точкой с запятой.

   Пример того, как разрешить подключение к Серверу администрирования только одному устройству:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"192.0.2.0" -t s
```

   Пример того, как разрешить нескольким устройствам подключаться к Серверу администрирования:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
```

4. Перезапустите службу Сервера администрирования.

Узнать, успешно настроен список разрешенных IP-адресов, можно в журнале событий Kaspersky Event Log на Сервере администрирования.

**Как изменить список разрешенных IP-адресов**

Вы можете изменить список разрешенных точно так же, как и при его создании. Для этого выполните ту же команду и укажите новый список разрешенных:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"<IP addresses>" -t s
```

Если вы хотите удалить некоторые IP-адреса из списка разрешенных, перепишите его. Например, ваш список разрешенных включает следующие IP-адреса: 192.0.2.0; 198.51.100.0; 203.0.113.0. Вы хотите удалить IP-адрес 198.51.100.0. Для этого в командной строке введите следующую команду:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"192.0.2.0; 203.0.113.0" -t s
```

Не забудьте перезапустить службу Сервера администрирования.

**Как сбросить настроенный список разрешенных IP-адресов**

► *Чтобы сбросить уже настроенный список разрешенных IP-адресов:*

1. Введите следующую команду в командной строке с правами администратора:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
"" -t s
```

2. Перезапустите службу Сервера администрирования.

После этого IP-адреса больше не проверяются.

## Использование утилиты klscflag для закрытия порта 13291

Порт 13291 Сервера администрирования используется для приема подключений от Консолей администрирования. По умолчанию порт открыт. Если вы не хотите использовать Консоль администрирования на основе консоли Microsoft Management Console (MMC) или утилиту klakaut, вы можете закрыть этот порт с помощью утилиты klscflag. Эта утилита изменяет значение параметра KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

► *Чтобы закрыть порт 13291:*

1. Выполните следующую команду в командной строке:

```
klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN
-sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

2. Перезапустите службу Сервера администрирования Kaspersky Security Center.

Порт 13291 закрыт.

► *Чтобы проверить, был ли успешно закрыт порт 13291:*

Выполните следующую команду в командной строке:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN
-svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Эта команда возвращает следующий результат:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Значение `false` означает, что порт закрыт. В противном случае отображается значение `true`.

См. также:

Порты, используемые программой Kaspersky Security Center 14.2 Web Console.....946

## Отключение от Сервера администрирования

► *Чтобы отключиться от Сервера администрирования:*

1. В дереве консоли выберите узел, соответствующий Серверу администрирования, от которого нужно отключиться.
2. В контекстном меню узла выберите пункт **Отключиться от Сервера администрирования**.

## Добавление Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли Сервер администрирования:*

1. В главном окне программы Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. В контекстном меню узла выберите пункт **Новый → Сервер администрирования**.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя устройства> (Не подключен)**, с которого вы можете подключиться к любому из установленных в сети Серверов администрирования.

## Удаление Сервера администрирования из дерева консоли

► *Чтобы удалить Сервер администрирования из дерева консоли:*

1. В дереве консоли выберите узел, соответствующий удаляемому Серверу администрирования.
2. В контекстном меню узла выберите пункт **Удалить**.

## Добавление виртуального Сервера администрирования в дерево консоли

► *Чтобы добавить в дерево консоли виртуальный Сервер администрирования:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать виртуальный Сервер администрирования.
2. В узле Сервера администрирования выберите папку **Серверы администрирования**.
3. В рабочей области папки **Серверы администрирования** перейдите по ссылке **Добавить виртуальный Сервер администрирования**.

   Запустится мастер создания виртуального Сервера администрирования.
4. В окне **Имя виртуального Сервера администрирования** укажите имя создаваемого виртуального Сервера.

   Имя виртуального Сервера администрирования не может превышать 255 символов и содержать специальные символы ("*<>?\:|).
5. В окне **Ввод адреса подключения устройств к виртуальному Серверу** укажите адрес подключения устройств.

Адрес подключения виртуального Сервера администрирования – это сетевой адрес, по которому к нему будут подключаться устройства. Адрес подключения состоит из двух частей: сетевого адреса физического Сервера администрирования и имени виртуального Сервера, разделенных символом косой черты (слешем). Имя виртуального Сервера будет подставлено автоматически. Указанный адрес будет использоваться на этом виртуальном Сервере как адрес по умолчанию в инсталляционных пакетах Агента администрирования.

6. В окне **Создание учетной записи администратора виртуального Сервера** назначьте администратором виртуального Сервера пользователя из списка или добавьте новую учетную запись для администратора по кнопке **Создать**.

   Вы можете указать несколько учетных записей.

В результате в дереве консоли будет создан узел с именем **Сервер администрирования – <Имя виртуального Сервера>**.

## Смена учетной записи службы Сервера администрирования. Утилита klsrvswch

Если вам требуется изменить учетную запись службы Сервера администрирования, заданную при установке программы Kaspersky Security Center, вы можете воспользоваться утилитой смены учетной записи Сервера администрирования klsrvswch.

При установке Kaspersky Security Center утилита автоматически копируется в папку установки программы.

Количество запусков утилиты не ограничено.

Утилита klsrvswch позволяет менять тип учетной записи. Например, если вы используете локальную учетную запись, вы можете сменить ее на доменную учетную запись либо на управляемую учетную запись службы (и наоборот). Утилита klsrvswch не позволяет изменить тип учетной записи на групповую управляемую учетную запись службы (gMSA).

Windows Vista и более поздние версии Windows не позволяют использовать учетную запись LocalSystem для Сервера администрирования. В этих версиях операционных систем Windows учетная запись **LocalSystem** неактивна.

► *Чтобы изменить учетную запись службы Сервера администрирования на доменную учетную запись:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись LocalSystem**.

В результате работы мастера учетная запись Сервера администрирования изменяется. Служба Сервера администрирования запустится под учетной записью *LocalSystem* и будет использовать ее учетные данные.

Для правильной работы Kaspersky Security Center требуется, чтобы учетная запись для запуска службы Сервера администрирования обладала правами администратора ресурса для размещения информационной базы Сервера администрирования.

► *Чтобы изменить учетную запись службы Сервера администрирования на учетную запись пользователя или на управляемую учетную запись службы:*

1. Запустите утилиту klsrvswch из папки установки Kaspersky Security Center.

   В результате запускается мастер изменения учетной записи службы Сервера администрирования. Следуйте далее указаниям мастера.

2. В окне **Учетная запись службы Сервера администрирования** выберите **Учетная запись пользователя**.
3. Нажмите на кнопку **Найти**.

   Откроется окно **Выбор пользователя**.

4. В окне **Выбор пользователя** нажмите на кнопку **Типы объекта**.
5. В списке типов объекта выберите **Пользователи** (если вы хотите использовать учетную запись пользователя) или **Учетная запись для служб** (если вы хотите использовать управляемую учетную запись службы) и нажмите на кнопку **ОК**.
6. В поле для имени объекта введите имя учетной записи или часть имени и нажмите на кнопку **Проверить имена**.
7. В списке соответствующих имен выберите необходимое имя и нажмите на кнопку **ОК**.
8. Если вы выбрали **Учетные записи служб**, в окне **Пароль учетной записи**, оставьте поля **Пароль** и **Подтверждение пароля** пустыми. Если вы выбрали **Пользователи**, введите пароль для пользователя и подтвердите его.

Учетная запись службы Сервера администрирования будет запускаться под выбранной вами учетной записью.

При использовании Microsoft SQL-сервера в режиме аутентификации учетной записи пользователя средствами Windows требуется обеспечить доступ к базе данных. Учетная запись пользователя должна быть владельцем базы данных Kaspersky Security Center. По умолчанию требуется использовать схему dbo.

## Изменение учетных данных СУБД

Иногда может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

► *Чтобы изменить учетные данные СУБД в среде Windows с помощью утилиты klsrvswch.exe:*

1. Запустите утилиту klsrvswch, которая расположена в папке установки Kaspersky Security Center.
2. Нажимайте на кнопку **Далее** мастера, пока не дойдете до шага **Изменить учетные данные доступа к DBMS**.
3. На шаге **Изменение учетных данных СУБД** выполните следующие действия:
   - Выберите параметр **Применить новые учетные данные**.
   - Укажите новое имя учетной записи в поле **Учетная запись**.
   - Укажите новый пароль для учетной записи в поле **Пароль**.
   - Подтвердите новый пароль в поле **Подтвердить пароль**.

Вы должны указать учетные данные учетной записи, которая существует в СУБД.

4. Нажмите на кнопку **Далее**.

После завершения работы мастера учетные данные СУБД изменяются.

## Решение проблем с узлами Сервера администрирования

Дерево в левой панели Консоли администрирования содержит узлы, соответствующие Серверам администрирования. Вы можете добавить в дерево консоли столько Серверов администрирования, сколько вам нужно (на стр. 681).

Консоль управления Microsoft Management Console (MMC) сохраняет список узлов Сервера администрирования в дереве консоли в теневую копию файла .msc. Теневая копия этого файла хранится в папке %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ на устройстве, на котором установлена Консоль администрирования. Для каждого узла Сервера администрирования в файле содержится следующая информация:

- Адрес Сервера администрирования.
- Номер порта.
- Используется ли TLS.

  Этот параметр зависит от номера порта (на стр. 300), используемого для подключения Консоли администрирования к Серверу администрирования.
- Имя пользователя.
- Сертификат Сервера администрирования.

### Устранение неисправностей

При подключении Консоли администрирования к Серверу администрирования (на стр. 678) сохраненный локально сертификат сравнивается с сертификатом Сервера администрирования. Если сертификаты не совпадают, в Консоли администрирования возникает ошибка. Несовпадение сертификатов может произойти, например, при замене сертификата Сервера администрирования (на стр. 111). В этом случае необходимо повторно создать узел Сервер администрирования в консоли.

► *Чтобы повторно создать узел Сервера администрирования:*

1. Закройте окно Консоли администрирования Kaspersky Security Center.
2. Удалите файл Kaspersky Security Center 14.2 из папки %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Запустить Консоль администрирования Kaspersky Security Center.

   Отобразится предложение подключиться к Серверу администрирования и принять его существующий сертификат.
4. Выполните одно из следующих действий:
   - Примите существующий сертификат, нажав на кнопку **Да**.
   - Чтобы указать ваш сертификат, нажмите на кнопку **Нет** и перейдите к файлу сертификата, используемого для аутентификации Сервера администрирования.

Проблема с сертификатом решена. Вы можете использовать Консоль администрирования для подключения к Серверу администрирования.

## Просмотр и изменение параметров Сервера администрирования

Вы можете настраивать параметры Сервера администрирования в окне свойств Сервера администрирования.

► *Чтобы открыть окно Свойства: Сервер администрирования,*

в контекстном меню узла Сервера администрирования в дереве консоли выберите пункт **Свойства**.

### В этом разделе



### Настройка общих параметров Сервера администрирования

Вы можете настраивать общие параметры Сервера администрирования в разделах **Общие**, **Параметры**, **Хранение событий**, и **Безопасность** окна свойств Сервера администрирования.

Раздел **Безопасность** не отображается в окне свойств Сервера администрирования, если его отображение выключено в интерфейсе Консоли администрирования.

► *Чтобы включить отображение раздела **Безопасность** в Консоли администрирования:*

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок **Отображать разделы с параметрами безопасности** и нажмите на кнопку **ОК**.
4. В окне с сообщением программы нажмите на кнопку **ОК**.

Раздел **Безопасность** отобразится в окне свойств Сервера администрирования.

### Параметры интерфейса Консоли администрирования

Вы можете настроить параметры интерфейса Консоли администрирования для отображения или скрытия элементов управления пользовательского интерфейса, связанных со следующими функциями:

- Системное администрирование.
- Шифрование и защита данных

- Параметры контроля рабочего места.
- Управление мобильными устройствами
- Подчиненные Серверы администрирования.
- Разделы с параметрами безопасности.

► *Чтобы настроить параметры интерфейса Консоли администрирования:*

1. В дереве консоли выберите требуемый Сервер администрирования.
2. В меню **Вид** главного окна программы выберите пункт **Настройка интерфейса**.
3. В открывшемся окне **Настройка интерфейса** установите флажок рядом с функциональностью, которая должна отображаться, и нажмите на кнопку **ОК**.
4. В окне с сообщением программы нажмите на кнопку **ОК**.

Выбранная функциональность отображается в интерфейсе Консоли администрирования.

## Обработка и хранение событий на Сервере администрирования

Информация о событиях в работе программы и управляемых устройств сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, программа может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программы вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые. Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

Можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

kaspersky

## Просмотр журнала подключений к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к Серверу администрирования.

► *Чтобы настроить регистрацию событий подключения к Серверу администрирования:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить регистрацию событий подключения.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования, в разделе **Параметры подключения к Серверу администрирования**, выберите подраздел **Порты подключения**.
4. Включите параметр **Регистрация событий подключения к Серверу администрирования**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

## Контроль возникновения вирусных эпидемий

Kaspersky Security Center позволяет вам своевременно реагировать на возникновение угроз вирусных эпидемий. Оценка угрозы вирусной эпидемии производится путем контроля вирусной активности на устройствах.

Вы можете настраивать правила оценки угрозы вирусной эпидемии и действия в случае ее возникновения в разделе **Вирусная атака** окна свойств Сервера администрирования.

Порядок оповещения о событии *Вирусная атака* можно задать в разделе **Настройка событий** окна свойств Сервера администрирования (на стр. 686), в окне свойств события *Вирусная атака*.

Событие *Вирусная атака* формируется при возникновении событий *Обнаружен вредоносный объект* в работе программ безопасности. Поэтому для распознавания вирусной эпидемии информацию о событиях *Обнаружен вредоносный объект* требуется сохранять на Сервере администрирования.

Параметры сохранения информации о событии *Обнаружен вредоносный объект* задаются в политиках программ безопасности.

При подсчете событий *Обнаружен вредоносный объект* учитывается только информация с устройств главного Сервера администрирования. Информация с подчиненных Серверов администрирования не учитывается. Для каждого подчиненного Сервера параметры события *Вирусная атака* требуется настраивать индивидуально.

## См. также:

Сценарий: Мониторинг и отчеты .....576

kaspersky

## Ограничение трафика

Для снижения трафика в сети предусмотрена возможность ограничения скорости передачи данных на Сервер администрирования с отдельных IP-диапазонов и IP-интервалов.

Вы можете создавать и настраивать правила ограничения трафика в разделе **Трафик** окна свойств Сервера администрирования.

► *Чтобы создать правила ограничения трафика:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования, для которого нужно создать правила ограничения трафика.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Трафик**.
4. Нажмите на кнопку **Добавить**.
5. В окне **Новое правило** настройте следующие параметры:

   В блоке **Интервал IP-адресов, для которых нужно ограничивать трафик** можно выбрать способ задания подсети или диапазона, для которого ограничивается скорость передачи, и указать значения параметров для выбранного способа. Выберите один из следующих способов:

   - **Задать интервал адресом и маской подсети**

     Трафик ограничивается по параметрам подсети. Укажите в полях ввода адрес подсети и маску подсети для определения интервала, в пределах которого будет ограничен трафик.

     Нажмите на кнопку **Обзор**, чтобы добавить подсеть из глобального списка подсетей (на стр. 935).

   - **Задать интервал начальным и конечным IP-адресом**

     Трафик ограничивается по интервалу IP-адресов. Укажите интервал IP-адресов в полях ввода **Начальный IP-адрес** и **Конечный IP-адрес**.

     По умолчанию этот вариант выбран.

   В блоке **Ограничение трафика** можно настроить следующие параметры ограничения скорости передачи данных:

   - **Период**

     Временной интервал, во время которого будет действовать ограничение трафика. Границы временного интервала можно указать в полях ввода.

   - **Ограничение (КБ/сек)**

     Предельное значение суммарной скорости передачи входящих и исходящих данных Сервера администрирования. Ограничение действует только в течение временного интервала, заданного в поле **Период**.

   - **Ограничивать трафик на оставшееся время (КБ/сек)**

     Трафик ограничивается не только в течение интервала, указанного в поле **Период**, но и в остальное время.

     По умолчанию флажок снят. Значение поля может не совпадать со значением поля **Ограничение (КБ/сек)**.

В первую очередь правила ограничения трафика влияют на передачу файлов. Эти правила не применяются к трафику, который возникает при синхронизации между Сервером администрирования и Агентом администрирования, или между главным Сервером администрирования и подчиненным Сервером администрирования.

### Настройка параметров Веб-сервера

Веб-сервер используется для публикации автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

Вы можете настроить параметры подключения Веб-сервера к Серверу администрирования и задать сертификат Веб-сервера в разделе **Веб-сервер** окна свойств Сервера администрирования.

### Работа с внутренними пользователями

Учетные записи *внутренних пользователей* используются для работы с виртуальными Серверами администрирования. В программе Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

Вы можете настраивать параметры учетных записей внутренних пользователей в папке **Учетные записи пользователей** дерева консоли(на стр. 765).

## Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security. Поэтому не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

Мастер первоначальной настройки программы создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Если в качестве СУБД используется экземпляр Microsoft SQL Server, установленный на другом устройстве, следует изменить задачу резервного копирования: указать в качестве папки для хранения сделанных резервных копий UNC-путь, доступный на запись как службе Сервера администрирования, так и службе SQL Server. Это неочевидное требование является следствием особенности резервного копирования в СУБД Microsoft SQL Server.

Если в качестве СУБД используется локальный экземпляр Microsoft SQL Server, также рекомендуется сохранять резервные копии на отдельном носителе, чтобы обезопасить их от повреждения одновременно с Сервером администрирования.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Если вы используете Microsoft SQL Server в качестве СУБД, вы можете минимизировать размер резервных копий. Для этого установите флажок **Сжимать резервные копии (Compress backup)** в параметрах SQL Server.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Инсталляция Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа (например, тот же SQL Server или MariaDB) той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

## В этом разделе



## Использование снимка файловой системы для уменьшения времени резервного копирования

В Kaspersky Security Center уменьшено по сравнению с более ранними версиями время простоя Сервера администрирования во время резервного копирования данных. Кроме того, в параметры задачи добавлена функция **Использовать моментальный снимок файловой системы для резервного копирования данных**. Эта функция позволяет дополнительно уменьшить время простоя за счет того, что утилита klbackup создает при выполнении резервного копирования теневую копию диска (это занимает несколько секунд) и одновременно производит копирование базы данных (это занимает не более нескольких минут). Создав теневую копию диска и сделав копию базы данных, klbackup снова делает Сервер администрирования доступным для соединения.

Вы можете пользоваться функцией создания снимка файловой системы только при соблюдении двух условий:

- Папка общего доступа Сервера администрирования и папка %ALLUSERSPROFILE%\KasperskyLab находятся на одном логическом диске и локальны по отношению к Серверу администрирования.
- Внутри папки %ALLUSERSPROFILE%\KasperskyLab нет созданных вручную символических ссылок.

Не используйте функцию, если хотя бы одно из этих условий не выполняется. В ответ на попытку создать снимок файловой системы программа выдаст сообщение об ошибке.

Для использования функции необходимо иметь учетную запись с правами на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%. Учетная запись службы сервера администрирования не имеет таких прав.

► *Чтобы воспользоваться функцией создания снимка файловой системы для уменьшения времени резервного копирования:*

1. В разделе **Задачи** выберите задачу резервного копирования.
2. В контекстном меню выберите пункт **Свойства**.
3. В отобразившемся окне свойств задачи выберите раздел **Параметры**.
4. Установите флажок **Использовать моментальный снимок файловой системы для резервного копирования данных**.
5. В полях **Имя пользователя** и **Пароль** введите имя и пароль от учетной записи, имеющей право на создание снимков логического диска, на котором расположена папка %ALLUSERSPROFILE%.
6. Нажмите на кнопку **Применить**.

При следующих запусках задачи резервного копирования утилита klbackup будет создавать снимки файловой системы, и время простоя Сервера администрирования во время выполнения задачи уменьшится.

## Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Новому Серверу назначить тот же самый адрес: NetBIOS-имя, FQDN-имя, статический IP – смотря по тому, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

## Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.

3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Из меню **Пуск** запустить утилиту резервного копирования klbackup и выполнить восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенной программы Kaspersky Security Center и, как следствие, неправильная работа программы.

## Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Обратите внимание, что резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых программ.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных (см. стр. 693) через Консоль администрирования.
- Запустить утилиту klbackup (см. стр. 693) на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

kaspersky

## В этом разделе



## Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования:*

1. В дереве консоли выберите папку **Задачи**.
2. Запустите процесс создания одним из следующих способов:
   - В контекстном меню папки дерева консоли **Задачи** выберите пункт **Новый** → **Задача**.
   - По кнопке **Создать задачу** в рабочей области.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера **Тип задачи** выберите тип задачи **Резервное копирование данных Сервера администрирования**.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи.

## Утилита резервного копирования и восстановления данных (klbackup)

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

Утилита klbackup может работать в двух режимах:

- интерактивный (см. стр. 693);
- неинтерактивный (см. стр. 696).

## Резервное копирование и восстановление данных в интерактивном режиме

► *Чтобы создать резервную копию данных Сервера администрирования в интерактивном режиме:*

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

2. В первом окне мастера выберите пункт **Выполнить резервное копирование данных Сервера администрирования**.

   При включении параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет сохранена только резервная копия сертификата Сервера администрирования.

   Нажмите **Далее**.

3. В следующем окне мастера укажите параметры:

   - **Целевая папка для резервной копии данных**
   - **Перенос данных в формате MySQL/MariaDB**
   - **Перенести в формат Azure**
   - **Включать текущую дату и время в имя папки назначения для резервных копий**
   - **Пароль для резервной копии данных**

4. Нажмите на кнопку **Далее** для выполнения резервного копирования.

5. Если вы работаете с базой данных в облачном окружении, таком как Amazon Web Services (AWS) или Microsoft Azure, заполните следующие поля в окне **Войти в онлайн-хранилище**:

   - Для AWS:
     - **Имя корзины S3**

       Имя корзины S3, которое вы создали для резервной копии данных.

     - **ID ключа доступа**

       Вы получили ID ключа (последовательность из букв и цифр), когда создали учетную запись IAM-пользователя для работы с корзиной S3 в хранилище инстансов.

       Поле доступно, если вы выбрали базу RDS для контейнера S3.

     - **Секретный ключ**

       Секретный ключ, который вы получили с ID ключа доступа при создании учетной записи IAM-пользователя.

       Символы секретного ключа отображаются в виде звездочек. После того, как вы начали вводить секретный ключ, отображается кнопка **Показать**. Нажмите на эту кнопку и удерживайте ее необходимое вам время, чтобы просмотреть введенные символы.

       Поле доступно, если вы выбрали для авторизации ключ доступа AWS IAM, а не IAM-роль.

   - Для Microsoft Azure:
     - **Имя учетной записи хранения Azure**

       Вы создали имя учетной записи хранения Azure для работы с Kaspersky Security Center.

     - **Идентификатор подписки Azure**

       Вы создали подписку на портале Azure.

     - **Пароль Azure**

       Вы получили пароль к идентификатору приложения при создании идентификатора приложения в Azure.

Символы пароля отображаются в виде звездочек. После того, как вы начали вводить пароль, отображается кнопка **Показать**. Нажмите и удерживайте эту кнопку, чтобы просмотреть введенные символы.

- **Идентификатор приложения в Azure**

  Вы создали этот идентификатор приложения на портале Azure.

  Вы можете указать только один идентификатор приложения в Azure для опроса и других целей. Если необходимо опрашивать другой сегмент Azure, вы должны сначала удалить первый сегмент в существующем соединении Azure.

- **Имя SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Группа источника SQL-сервера Azure**

  Имя и группа источника доступны в свойствах SQL-сервера Azure.

- **Ключ доступа хранилища Azure**

  Доступен в свойствах учетной записи хранения в разделе "Access Keys". Вы можете использовать любой ключ (key1 или key2).

► *Чтобы восстановить данные Сервера администрирования в интерактивном режиме:*

1. Запустите утилиту klbackup, расположенную в папке установки Kaspersky Security Center. Запустите утилиту под той же учетной записью, под которой был установлен Сервер администрирования. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

   В результате запустится мастер выполнения резервного копирования и восстановления данных.

2. В первом окне мастера выберите пункт **Выполнить восстановление данных Сервера администрирования**.

   При включении параметра **Выполнять резервное копирование и восстановление только для сертификата Сервера администрирования** будет восстановлен только сертификат Сервера администрирования.

   Нажмите **Далее**.

3. В окне мастера **Параметры восстановления**:

   - Укажите папку, содержащую резервную копию данных Сервера администрирования.

     Если вы работаете в облачном окружении, таком как AWS или Azure, укажите адрес хранилища. Также убедитесь, что файл называется backup.zip.

   - Укажите пароль, введенный при резервном копировании данных.

     При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке.

4. Нажмите на кнопку **Далее** для восстановления данных.

## См. также:

Резервное копирование и восстановление данных в неинтерактивном режиме .....696

## Резервное копирование и восстановление данных в неинтерактивном режиме

► *Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в неинтерактивном режиме,*

в командной строке устройства, на котором установлен Сервер администрирования, запустите утилиту klbackup с необходимым набором ключей.

Синтаксис командной строки утилиты:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD] [-online]
```

> Если не задать пароль в командной строке утилиты klbackup, утилита запросит его ввод интерактивно.

Описания ключей:

- `-path BACKUP_PATH` – сохранить информацию в папке BACKUP_PATH / использовать для восстановления данные из папки BACKUP_PATH (обязательный параметр).
- `-logfile LOGFILE` – сохранить отчет о копировании или восстановлении данных Сервера администрирования.

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке BACKUP_PATH.
- `-use_ts` – при сохранении данных копировать информацию в папку BACKUP_PATH, во вложенную папку с именем, отображающим текущую системную дату и время операции в формате `klbackup ГГГГ-ММ-ДД # ЧЧ-ММ-СС`. Если ключ не задан, информация сохраняется в корне папки BACKUP_PATH.

  При попытке сохранить информацию в папку, в которой уже есть резервная копия, появится сообщение об ошибке. Обновление информации не произойдет.

  Наличие ключа `-use_ts` позволяет вести архив данных Сервера администрирования. Например, если ключом `-path` была задана папка `C:\KLBackups`, то в папке `klbackup 2022-06-19 # 11-30-18`, сохранится информация о состоянии Сервера администрирования на дату 19 июня 2022 года, 11 часов 30 минут 18 секунд.
- `-restore` – выполнить восстановление данных Сервера администрирования. Восстановление данных осуществляется на основании информации, представленной в папке BACKUP_PATH. Если ключ отсутствует, производится резервное копирование данных в папку BACKUP_PATH.
- `-password PASSWORD` – сохранить или восстановить сертификат Сервера администрирования; для шифрования и расшифровки сертификата использовать пароль, заданный параметром PASSWORD.

  > Забытый пароль не может быть восстановлен. Требования к паролю отсутствуют. Длина пароля не ограничена, также возможна нулевая длина пароля (то есть без пароля).

При восстановлении данных необходимо указать тот же пароль, который был введен во время резервного копирования. Если после резервного копирования путь к общей папке изменился, проверьте работу задач, использующих восстановленные данные (задачи восстановления и задачи удаленной установки). При необходимости отредактируйте параметры этих задач. Пока данные восстанавливаются из файла резервной копии, никто не должен иметь доступ к общей папке Сервера администрирования. Учетная запись, под которой запускается утилита klbackup, должна иметь полный доступ к общей папке. Рекомендуется запускать утилиту на только что установленном Сервере администрирования.

- `-online` – создать резервную копию данных Сервера администрирования, создав моментальный снимок, чтобы минимизировать время автономного состояния Сервера администрирования. Если вы используете утилиту резервного копирования и восстановления данных, этот параметр игнорируется.

## Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер баз данных на новое устройство.
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

*Чтобы перенести Сервер администрирования на новое устройство:*

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

   Для этого запустите задачу резервного копирования данных (см. стр. 693) с помощью Kaspersky Security Center 14 Web Console или запустите утилиту klbackup (см. стр. 693).

   Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на MySQL или MariaDB. Чтобы создать резервную копию данных, запустите утилиту klbackup в интерактивном режиме (см. стр. 693). Включите параметр **Перенос данных в формате MySQL/MariaDB** в окне **Параметры резервного копирования** мастера выполнения резервного копирования и восстановления данных. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.
   Также можно включить параметр **Перенос в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL (см. стр. ).

2. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям (см. стр. 69) для Сервера администрирования, Консоли администрирования и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования доступны (см. стр. 98).
3. На новом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования.

   При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.

4. Запустите выборочную установку Сервера администрирования (см. стр. 243) на новом устройстве.

5. Установите компоненты Сервера администрирования в ту же папку (см. стр. 245), где Сервер администрирования установлен на предыдущем устройстве. Нажмите на кнопку **Обзор**, чтобы указать путь к файлу.

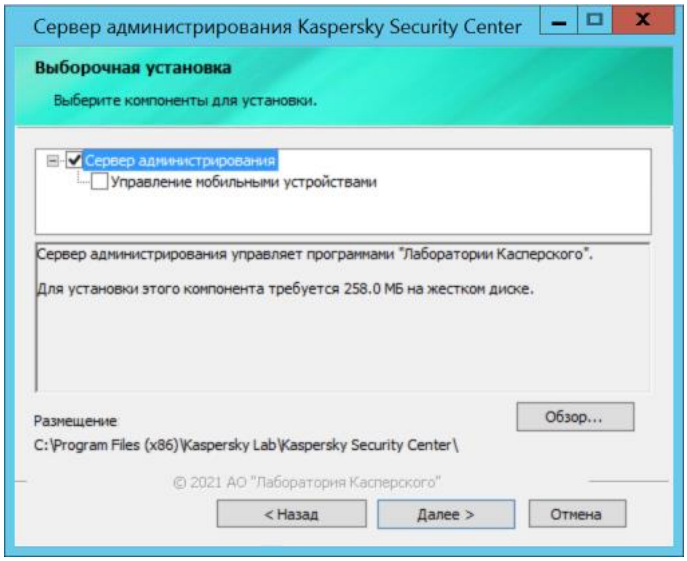



Figure 2. Окно **Выборочная установка**

6. Настройте параметры подключения к серверу базы данных (см. стр. 247).

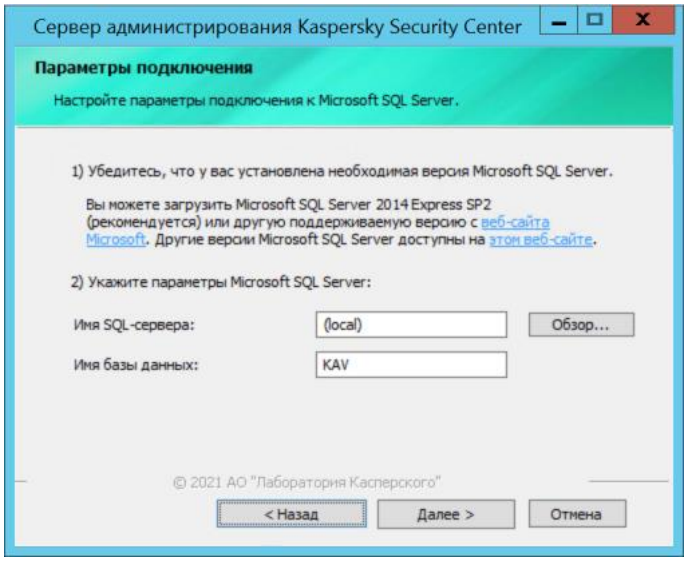



Figure 3. Окно **Параметры подключения**

В зависимости от того, где нужно разместить сервер базы данных, выполните одно из следующих действий:

- Переместите сервер базы данных на новое устройство.
- Оставьте сервер базы данных на предыдущем устройстве.

7. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup (см. стр. 693).

Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

8. Запустите Консоль администрирования и подключитесь к Серверу администрирования (см. стр. 674).
9. Убедитесь, что все клиентские устройства подключены к Серверу администрирования.
10. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Kaspersky Security Center 14.2 Web Console (см. стр. 1004) для переноса Сервера администрирования и сервера баз данных на другое устройство.

### См. также:



## Избегание конфликтов между Серверами администрирования

Если в сети имеется несколько Серверов администрирования, они могут видеть одни и те же клиентские устройства. Это может привести к тому, что, например, несколько Серверов администрирования будут выполнять удаленную установку одной и той же программы на одно устройство, а также к другим конфликтам. Чтобы избежать такой ситуации, в Kaspersky Security Center 11 можно запретить установку программы на устройство, управляемое другим Сервером администрирования (на стр. 365).

Свойство **Под управлением другого Сервера администрирования** можно также использовать как критерий для следующих операций:

- Поиск устройств (см. стр. 907)
- Выборки устройств (см. стр. 603).
- Правила перемещения устройств (см. стр. 445).
- Автоматического назначения тегов (см. стр. 733).

В Kaspersky Security Center используется эвристический подход для определения, какой Сервер администрирования управляет клиентским устройством: тот, на котором вы работаете, или другой.

## Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Консоли администрирования или Kaspersky Security Center 14.2 Web Console.

kaspersky

## В этом разделе



## Сценарий: Настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, программа сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

**Предварительные требования**

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение проверки подлинности.

**Этапы**

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

a. **Установка приложения проверки подлинности на устройство**

   Вы можете установить Google Authenticator, Microsoft Authenticator или любое другое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени.

b. **Синхронизация времени приложения проверки подлинности и время устройства, на котором установлен Сервер администрирования**

   Убедитесь, что время, установленное в приложении проверки подлинности, синхронизировано со временем Сервера администрирования.

c. **Включение двухэтапной проверки и получение секретного ключа для своей учетной записи**

   Инструкции:

Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для вашей учетной записи (см. стр. 703)

Для Kaspersky Security Center 14.2 Web Console: Включение двухэтапной проверки для вашей учетной записи (см. стр. 999)

После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

**d. Включение двухэтапной проверки для всех пользователей**

Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

Инструкции:

Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для всех пользователей (см. стр. 704)

Для Kaspersky Security Center 14.2 Web Console: Включение двухэтапной проверки для всех пользователей (см. стр. 1000)

**e. Изменение имени издателя кода безопасности**

Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

Инструкции:

Для Консоли администрирования на основе MMC: Изменение имени издателя кода безопасности (см. стр. 707)

Для Kaspersky Security Center 14.2 Web Console: Изменение имени издателя кода безопасности (см. стр. 1003)

**f. Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку**

При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

Инструкции:

Для Консоли администрирования на основе MMC: Исключение учетных записей из двухэтапной проверки (см. стр. 706)

Для Kaspersky Security Center 14.2 Web Console: Исключение учетных записей из двухэтапной проверки (см. стр. 1001)

**Результаты**

После выполнения этого сценария:

- Двухэтапная проверка для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

## См. также:

kaspersky

## О двухэтапной проверке

Kaspersky Security Center предоставляет двухэтапную проверку для пользователей Консоли администрирования или Kaspersky Security Center 14.2 Web Console. Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Консоль администрирования или Kaspersky Security Center 14.2 Web Console вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию (на стр. 979) для своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Чтобы получить одноразовый код безопасности, вы должны установить приложение проверки подлинности на своем компьютере или мобильном устройстве.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении проверки подлинности. Вы можете изменить имя издателя кода безопасности. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Имя издателя используется в качестве идентификатора Сервера администрирования в приложении проверки подлинности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению проверки подлинности. Код безопасности является одноразовым и действует до 90 секунд (точное время может варьироваться).

Любой пользователь, для которого включена двухэтапная проверка, может повторно ввести свой секретный ключ. Когда пользователь выполняет аутентификацию с повторно выданным секретным ключом и использует этот ключ для входа в программу, Сервер администрирования сохраняет новый секретный ключ для учетной записи пользователя. Если пользователь неправильно ввел новый секретный ключ, Сервер администрирования не сохраняет новый секретный ключ и оставляет текущий секретный ключ действующим для дальнейшей аутентификации.

Любое программное обеспечение для аутентификации, которое поддерживает алгоритм одноразового пароля на основе времени (TOTP), может использоваться в качестве приложения проверки подлинности. Например, Google Authenticator. Чтобы сгенерировать код безопасности, вы должны синхронизировать время, установленное в приложении проверки подлинности, со временем, установленным для Сервера администрирования.

Приложение проверки подлинности генерирует секретный код следующим образом:

1. Сервер администрирования генерирует специальный секретный ключ и QR-код.
2. Вы передаете сгенерированный секретный ключ или QR-код приложению проверки подлинности.
3. Приложение проверки подлинности генерирует одноразовый код безопасности, который вы передаете в окно аутентификации Сервера администрирования.

Рекомендуется установить приложение проверки подлинности на несколько мобильных устройств. Сохраните секретный ключ (или QR-код) и храните его в надежном месте. Это поможет вам восстановить доступ к Консоли администрирования или Kaspersky Security Center 14.2 Web Console в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Kaspersky Security Center, вы можете включить двухэтапную проверку для своей учетной записи и включить двухэтапную проверку для всех пользователей.

Вы можете исключить (на стр. 1001) учетные записи из двухэтапной проверки. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Двухэтапная проверка работает в соответствии со следующими правилами:

- Только пользователь с правом Изменение списков управления доступом объектов (см. стр. 771) функциональной области **Общий функционал**: **Права пользователей**, может включать двухэтапную проверку для всех пользователей.
- Только пользователь, включивший двухэтапную проверку для своей учетной записи, может включить двухэтапную проверку для всех пользователей.
- Только пользователь, включивший двухэтапную проверку для своей учетной записи, может исключить другие учетные записи пользователей из списка двухэтапной проверки, включенной для всех пользователей.
- Пользователь может включить двухэтапную проверку только для своей учетной записи.
- Пользователь, у которого есть право Изменение списков управления доступом объектов (см. стр. 771) функциональной области **Общий функционал**: **Права пользователей** и, который авторизован в Консоли администрирования или в Kaspersky Security Center 14.2 Web Console с помощью двухэтапной проверки, может выключать двухэтапную проверку: для любого другого пользователя, только если двухэтапная проверка для всех пользователей выключена; для пользователя, исключенного из списка двухэтапной проверки включенной для всех пользователей.
- Любой пользователь, выполнивший вход в Консоль администрирования или Kaspersky Security Center 14.2 Web Console с помощью двухэтапной проверки, может повторно получить секретный ключ.
- Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, с которым вы сейчас работаете. Если вы включите этот параметр на Сервере администрирования, вы также включаете этот параметр для учетных записей пользователей его виртуальных Серверов администрирования (на стр. 169) и не включаете двухэтапную проверку для учетных записей пользователей подчиненных Серверов администрирования.

Если для учетной записи на Сервере администрирования Kaspersky Security Center версии 13 или выше включена двухэтапная проверка, то пользователь не сможет войти в программу Kaspersky Security Center Web Console версий 12, 12.1 или 12.2.

## См. также:

Исключение учетных записей из двухэтапной проверки .....706

## Включение двухэтапной проверки для вашей учетной записи

Перед тем как включить двухэтапную проверку для своей учетной записи, убедитесь, что на вашем мобильном устройстве установлено приложение проверки подлинности. Убедитесь, что время, установленное в приложении проверки подлинности, синхронизировано со временем Сервера администрирования.

► *Чтобы включить двухэтапную проверку для учетной записи:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы** и выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. В разделе **Двухэтапная проверка** нажмите на кнопку **Настроить**.

   В открывшемся окне двухэтапной проверки отобразится секретный ключ.
4. Введите секретный ключ в приложении проверки подлинности, чтобы получить одноразовый код безопасности Вы можете указать секретный ключ в приложении проверки подлинности вручную или отсканировать QR-код своим мобильным устройством.
5. Укажите код безопасности, сгенерированный приложением проверки подлинности и нажмите на кнопку **ОК**, чтобы закрыть окно двухэтапной проверки.
6. Нажмите на кнопку **Применить**.
7. Нажмите на кнопку **ОК**.

Двухэтапная проверка для вашей учетной записи включена.

## См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей .....700

## Включение двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для всех пользователей, программа откроет окно включения двухэтапной проверки для вашей учетной записи (на стр. 703).

► *Чтобы включить двухэтапную проверку для всех пользователей:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы**, выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Нажмите на кнопку **Установить как обязательную**, чтобы включить двухэтапную проверку для всех пользователей.
4. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **ОК**.

Двухэтапная проверка для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения этого параметра, необходимо настроить двухэтапную проверку для своих учетных записей, за исключением пользователей, учетные записи которых исключены (на стр. 706) из двухэтапной проверки.

## См. также:



## Выключение двухэтапной проверки для учетной записи пользователя

► *Чтобы выключить двухэтапную проверку для вашей учетной записи:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы**, выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. В разделе **Двухэтапная проверка** нажмите на кнопку **Выключить**.
4. Нажмите на кнопку **Применить**.
5. Нажмите на кнопку **ОК**.

Двухэтапная проверка для вашей учетной записи выключена.

Вы можете выключить двухэтапную проверку для других учетных записей пользователей. Эта защита используется, например, если пользователь потеряет или сломает мобильное устройство.

Вы можете выключить двухэтапную проверку для других учетных записей пользователей, только если у вас есть право Изменение списков управления доступом объектов (см. стр. 771) в области **Общий функционал**: **Права пользователей**. Следуя приведенным ниже инструкциям, вы также можете выключить двухэтапную проверку для своей учетной записи.

► *Чтобы выключить двухэтапную проверку для учетной записи любого пользователя:*

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.
2. В рабочей области папки нажмите на учетную запись пользователя, для которой вы хотите выключить двухэтапную проверку.
3. В открывшемся окне **Свойства:** В открывшемся окне **<Имя пользователя>** выберите раздел **Двухэтапная проверка**.
4. В разделе **Двухэтапная проверка** выберите следующие параметры:
   - Если вы хотите выключить двухэтапную проверку для всех пользователей, нажмите на кнопку **Выключить**.
   - Если вы хотите исключить эту учетную запись пользователя из двухэтапной проверки, выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.
5. Нажмите на кнопку **Применить**.
6. Нажмите на кнопку **ОК**.

Двухэтапная проверка учетной записи пользователя выключена.

## См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей .....700

## Выключение двухэтапной проверки для всех пользователей

Вы можете выключить двухэтапную проверку для всех пользователей Сервера администрирования, если у вас есть право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► *Чтобы выключить двухэтапную проверку для всех пользователей:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы**, выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Нажмите на кнопку **Установить как необязательную**, чтобы выключить двухэтапную проверку для всех пользователей.
4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.
5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Двухэтапная проверка для всех пользователей выключена.

## См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей .....700

## Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетную запись из двухэтапной проверки, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей**.

Если учетная запись пользователя исключена из двухэтапной проверки, этот пользователь может войти в Консоль администрирования или Kaspersky Security Center 14.2 Web Console без использования двухэтапной проверки.

Исключение учетных записей из двухэтапной проверки может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

► *Чтобы исключить учетную запись пользователя из двухэтапной проверки:*

1. Если вы хотите исключить учетную запись Active Directory, выполните опрос Active Directory (на стр. 329), чтобы обновить список пользователей Сервера администрирования.
2. В дереве консоли откройте папку **Учетные записи пользователей**.

Папка **Учетные записи пользователей** по умолчанию вложена в папку **Дополнительно**.

3. В рабочей области папки нажмите на учетную запись пользователя, которую вы хотите исключить из двухэтапной проверки.
4. В открывшемся окне **Свойства:** В открывшемся окне **<Имя пользователя>** выберите раздел **Двухэтапная проверка**.
5. В открывшемся разделе выберите параметр **Пользователь может пройти аутентификацию, используя только имя пользователя и пароль**.
6. В разделе **Двухэтапная проверка** нажмите на кнопку **Применить** и нажмите на кнопку **ОК**.

Эта учетная запись пользователя исключена из двухэтапной проверки. Вы можете проверить исключенные учетные записи в списке учетных записей пользователей (на стр. 765).

### См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей .....700

## Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению проверки подлинности.

► *Чтобы указать новое имя издателя кода безопасности:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования перейдите в панель **Разделы**, выберите раздел **Дополнительно**, а затем **Двухэтапная проверка**.
3. Укажите новое имя издателя кода безопасности в поле **Издатель кода безопасности**.
4. Нажмите на кнопку **Применить** в разделе **Двухэтапная проверка**.
5. Нажмите на кнопку **ОК** в разделе **Двухэтапная проверка**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

### См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей .....700

## Изменение общей папки Сервера администрирования

Общая папка Сервера администрирования указывается при установке Сервера администрирования. Месторасположение папки общего доступа можно изменить в свойствах Сервера администрирования.

► *Чтобы изменить общую папку:*

1. Назначьте права полного доступа для подгруппы **Everyone** для папки, которую вы хотите использовать как общую.
2. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
3. В окне свойства Сервера администрирования перейдите в раздел **Дополнительно** и выберите **Папка общего доступа Сервера администрирования**.
4. В разделе **Папка общего доступа Сервера администрирования** нажмите на кнопку **Изменить**.
5. Выберите папку, которую вы хотите использовать как общую.
6. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.
7. Назначить права на чтение для подгруппы **Everyone** для папки, которую вы выбрали как общую.

# Управление группами администрирования

Этот раздел содержит информацию о работе с группами администрирования.

Вы можете выполнять с группами администрирования следующие действия:

- добавлять в состав группы администрирования произвольное количество вложенных групп любых уровней иерархии;
- добавлять в состав групп администрирования устройства;
- изменять иерархию групп администрирования путем перемещения отдельных устройств и целых групп в другие группы;
- удалять из состава групп администрирования вложенные группы и устройства;
- добавлять в состав групп администрирования подчиненные и виртуальные Серверы администрирования;
- переносить устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера;
- определять, какие программы "Лаборатории Касперского" будут автоматически устанавливаться на устройства, включаемые в состав группы.

Эти действия можно выполнять, только если у вас есть права **Изменение** (на стр. 798) в области **Управление группами администрирования**, для групп, которыми вы хотите управлять (или для Сервера администрирования, к которому относятся эти группы).

## В этом разделе

## Создание групп администрирования

Иерархия групп администрирования формируется в главном окне программы Kaspersky Security Center в папке **Управляемые устройства**. Группы администрирования отображаются в виде папок в дереве консоли (см. рис. ниже).

Сразу после установки Kaspersky Security Center папка **Управляемые устройства** содержит только пустую папку **Серверы администрирования**.

> Наличие или отсутствие папки **Серверы администрирования** в дереве консоли определяется параметрами пользовательского интерфейса. Для включения отображения этой папки нужно перейти в меню **Вид → Настройка интерфейса** и в открывшемся окне **Настройка интерфейса** установить флажок **Отображать подчиненные Серверы администрирования**.

При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. В папку **Серверы администрирования** можно добавлять подчиненные и виртуальные Серверы администрирования.

Каждая созданная группа, как и папка **Управляемые устройства**, сначала содержит только пустую папку **Серверы администрирования** для работы с подчиненными и виртуальными Серверами администрирования этой группы. Информация о политиках и задачах этой группы, а также информация об устройствах, входящих в эту группу, отображается на закладках с соответствующими именами в рабочей области этой группы.

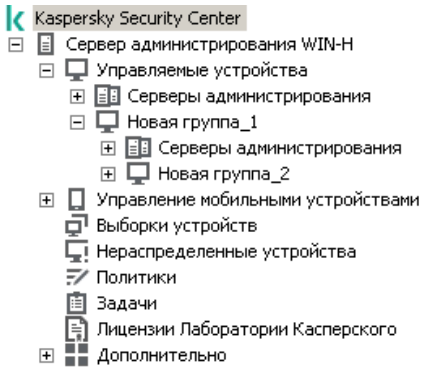



Figure 4. Просмотр иерархии групп администрирования

► *Чтобы создать группу администрирования:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. Если вы хотите создать подгруппу существующей группы администрирования, в папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой должна входить новая группа администрирования.

   Если вы создаете новую группу администрирования верхнего уровня иерархии, этот шаг можно пропустить.
3. Запустите процесс создания группы администрирования одним из следующих способов:
   - с помощью команды контекстного меню **Создать → Группу**;
   - по кнопке **Новая группа**, расположенной в рабочей области главного окна программы на закладке **Группы**.

4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем.

Программа позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► *Чтобы создать структуру групп администрирования:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи → Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

## Перемещение групп администрирования

Вы можете перемещать вложенные группы администрирования внутри иерархии групп.

Группа администрирования перемещается вместе со всеми вложенными группами, подчиненными Серверами администрирования, устройствами, групповыми политиками и задачами. К ней будут применены все параметры, соответствующие ее новому положению в иерархии групп администрирования.

Имя группы должно быть уникальным в пределах одного уровня иерархии. Если в папке, в которую вы перемещаете группу администрирования, уже существует группа с аналогичным названием, перед перемещением название группы следует изменить. Если вы предварительно не изменили название перемещаемой группы, к ее названию при перемещении автоматически добавляется окончание вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Невозможно изменить название группы **Управляемые устройства**, поскольку она является встроенным элементом Консоли администрирования.

► *Чтобы переместить группу в другую папку дерева консоли:*

1. Выберите перемещаемую группу в дереве консоли.
2. Выполните одно из следующих действий:
   - Переместите группу с помощью контекстного меню:
     1. В контекстном меню группы выберите пункт **Вырезать**.
     2. В контекстном меню группы администрирования, в которую нужно переместить выбранную группу, выберите пункт **Вставить**.
   - Переместите группу с помощью главного меню программы:
     a. Выберите пункт главного меню **Действие → Вырезать**.
     b. Выберите в дереве консоли группу администрирования, в которую нужно переместить выбранную группу.
     c. Выберите пункт главного меню **Действие → Вставить**.
   - Переместите группу в другую группу в дереве консоли с помощью мыши.

## Удаление групп администрирования

Вы можете удалить группу администрирования, если она не содержит подчиненных Серверов администрирования, вложенных групп и клиентских устройств и если для нее не сформированы задачи и политики.

Перед удалением группы администрирования требуется удалить из ее состава подчиненные Серверы администрирования, вложенные группы и клиентские устройства.

► *Чтобы удалить группу:*

1. В дереве консоли выберите группу администрирования.
2. Выполните одно из следующих действий:
   - в контекстном меню группы выберите пункт **Удалить**;
   - в главном меню программы выберите пункт **Действие → Удалить**;
   - Нажмите на кнопку **DELETE**.

## Автоматическое создание структуры групп администрирования

Kaspersky Security Center позволяет автоматически сформировать структуру групп администрирования с помощью мастера создания структуры групп.

Мастер создает структуру групп администрирования на основе следующих данных:

- структуры доменов и рабочих групп сети Windows;
- структуры групп Active Directory;
- содержимого текстового файла, созданного администратором вручную.

При формировании текстового файла требуется соблюдать следующие правила:

- Имя каждой новой группы должно начинаться с новой строки; разделитель должен начинаться с разрыва строки. Пустые строки игнорируются.

**Пример:**

Офис 1

Офис 2

Офис 3

В группе назначения будут созданы три группы первого уровня иерархии.

- Имя вложенной группы следует указывать через косую черту (/).

**Пример:**

Офис 1/Подразделение 1/Отдел 1/Группа 1

В группе назначения будут созданы четыре вложенные друг в друга подгруппы.

- Чтобы создать несколько вложенных групп одного уровня иерархии, следует указать "полный путь к группе".

**Пример:**

Офис 1/Подразделение 1/Отдел 1

Офис 1/Подразделение 2/Отдел 1

Офис 1/Подразделение 3/Отдел 1

Офис 1/Подразделение 4/Отдел 1

В группе назначения будет создана одна группа первого уровня иерархии "Офис 1", в состав которой будут входить четыре вложенные группы одного уровня иерархии "Подразделение 1", "Подразделение 2", "Подразделение 3", "Подразделение 4". В состав каждой из этих групп будет входить группа "Отдел 1".

Создание структуры групп администрирования с помощью мастера не нарушает целостности сети: новые группы добавляются, а не замещают существующие. Клиентское устройство не может быть включено в состав группы администрирования повторно, поскольку при перемещении устройства в группу администрирования оно удаляется из группы **Нераспределенные устройства**.

Если при создании структуры групп администрирования устройство по каким-либо причинам не было включено в состав группы **Нераспределенные устройства** (было выключено, отключено от сети), оно не будет автоматически перенесено в группу администрирования. Вы можете добавить устройства в группы администрирования вручную после завершения работы мастера.

► *Чтобы запустить автоматическое создание структуры групп администрирования:*

1. Выберите в дереве консоли папку **Управляемые устройства**.
2. В контекстном меню папки **Управляемые устройства** выберите пункт **Все задачи → Новая структура групп**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

## Автоматическая установка программ на устройства группы администрирования

Вы можете указать, какие инсталляционные пакеты нужно использовать для автоматической удаленной установки программ "Лаборатории Касперского" на вновь включенные в состав группы клиентские устройства.

► *Чтобы настроить автоматическую установку программ на новые устройства в группе администрирования:*

1. Выберите в дереве консоли нужную вам группу администрирования.
2. Откройте окно свойств этой группы администрирования.
3. В разделе **Автоматическая установка** выберите инсталляционные пакеты, которые следует устанавливать на новые устройства.
4. Нажмите на кнопку **ОК**.

Групповые задачи созданы. Эти задачи будут запускаться на клиентских устройствах сразу после их добавления в группу администрирования.

Если для автоматической установки указано несколько инсталляционных пакетов одной программы, задача установки будет создана только для последней версии программы.

# Управление клиентскими устройствами

Этот раздел содержит информацию о работе с клиентскими устройствами.

## В этом разделе

kaspersky

## Подключение клиентских устройств к Серверу администрирования

Подключение клиентского устройства к Серверу администрирования осуществляет Агент администрирования, установленный на клиентском устройстве.

При подключении клиентского устройства к Серверу администрирования выполняются следующие операции:

- Автоматическая синхронизация данных:
  - синхронизация списка программ, установленных на клиентском устройстве;
  - синхронизация политик, параметров программ, задач и параметров задач.
- Получение Сервером текущей информации о состоянии программ, выполнении задач и статистики работы программ.
- Доставка на Сервер информации о событиях, которые требуется обработать.

Автоматическая синхронизация данных производится периодически, в соответствии с параметрами Агента администрирования (например, один раз в 15 минут). Вы можете вручную задать интервал между соединениями.

Информация о событии доставляется на Сервер администрирования сразу после того, как событие произошло.

Если Сервер администрирования является удаленным, то есть находится вне сети организации, клиентские устройства подключаются к нему через интернет.

Для подключения устройств к Серверу администрирования через интернет должны быть выполнены следующие условия:

- Удаленный Сервер администрирования должен иметь внешний IP-адрес, и на нем должен быть открыт входящий порт 13000 (для подключения от Агентов администрирования). Рекомендуется также открыть порт UDP 13000 (для приема уведомлений о выключении устройств).
- На устройствах должны быть установлены Агенты администрирования.
- При установке Агента администрирования на устройства должен быть указан внешний IP-адрес удаленного Сервера администрирования. Если для установки используется инсталляционный пакет, внешний IP-адрес требуется указать вручную в свойствах инсталляционного пакета в разделе **Параметры**.
- Для управления программами и задачами устройства с помощью удаленного Сервера администрирования требуется установить флажок **Не разрывать соединение с Сервером администрирования** в окне свойств этого устройства в разделе **Общие**. После установки флажка необходимо дождаться синхронизации Сервера администрирования с удаленным устройством. Непрерывное соединение с Сервером администрирования могут поддерживать не более 300 клиентских устройств одновременно.

Для ускорения выполнения задач, поступающих от удаленного Сервера администрирования, можно открыть на устройстве порт 15000. В этом случае для запуска задачи Сервер администрирования посылает специальный пакет Агенту администрирования по порту 15000, не дожидаясь синхронизации с устройством.

Kaspersky Security Center позволяет настроить соединение клиентского устройства с Сервером администрирования таким образом, чтобы соединение не завершалось по окончании выполнения операций. Непрерывное соединение необходимо в том случае, если требуется постоянный контроль состояния программ, а Сервер администрирования не может инициировать соединение с клиентским устройством (например, соединение защищено сетевым экраном, запрещено открывать порты на клиентском устройстве, неизвестен IP-адрес клиентского устройства). Установить неразрывное соединение клиентского устройства с Сервером администрирования можно в окне свойств устройства, в разделе **Общие** .

Рекомендуется устанавливать непрерывное соединение с наиболее важными устройствами. Общее количество соединений, поддерживаемых Сервером администрирования одновременно, ограничено (до 300).

При синхронизации вручную используется вспомогательный способ подключения, при котором соединение инициирует Сервер администрирования. Перед подключением на клиентском устройстве требуется открыть UDP-порт. Сервер администрирования посылает на UDP-порт клиентского устройства запрос на соединение. В ответ на него производится проверка сертификата Сервера администрирования. Если сертификат Сервера совпадает с копией сертификата на клиентском устройстве, соединение осуществляется.

Запуск процесса синхронизации вручную используется также для получения текущей информации о состоянии программ, выполнении задач и статистике работы программ.

## Подключение клиентского устройства к Серверу администрирования вручную. Утилита klmover

Если вам требуется подключить клиентское устройство к Серверу администрирования вручную, вы можете воспользоваться утилитой klmover на клиентском устройстве.

При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

► *Чтобы подключить клиентское устройство к Серверу администрирования вручную с помощью утилиты klmover,*

на устройстве запустите утилиту klmover из командной строки.

При запуске из командной строки утилита klmover в зависимости от используемых ключей выполняет следующие действия:

- подключает Агент администрирования к Серверу администрирования с указанными параметрами;
- записывает результаты выполнения операции в файл журнала событий или выводит их на экран.

Синтаксис командной строки утилиты:

```
klmover [-logfile <имя файла>] [-address <адрес сервера>] [-pn <номер порта>] [-ps <номер SSL-порта>] [-nossl] [-cert <путь к файлу сертификата>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Для запуска утилиты требуются права администратора.

Описания ключей:

- `-logfile <имя файла>` – записать результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, результаты и сообщения об ошибках выводятся на экран.

- `-address <адрес сервера>` – адрес Сервера администрирования для подключения.

  В качестве адреса можно указать IP-адрес, NetBIOS- или DNS-имя устройства.

- `-pn <номер порта>` – номер порта, по которому будет осуществляться незашифрованное подключение к Серверу администрирования.

  По умолчанию установлен порт 14000.

- `-ps <номер SSL-порта>` – номер SSL-порта, по которому осуществляется зашифрованное подключение к Серверу администрирования с использованием протокола SSL.

  По умолчанию установлен порт 13000.

- `-nossl` – использовать незашифрованное подключение к Серверу администрирования.

  Если ключ не используется, подключение Агента администрирования к Серверу осуществляется по защищенному SSL-протоколу.

- `-cert <путь к файлу сертификата>` – использовать указанный файл сертификата для аутентификации доступа к Серверу администрирования.

  Если ключ не используется, Агент администрирования получает сертификат при первом подключении к Серверу администрирования.

- `-silent` – запустить утилиту на выполнение в неинтерактивном режиме.

  Использование ключа может быть полезно, например, при запуске утилиты из сценария входа при регистрации пользователя.

- `-dupfix` – ключ используется в случае, если установка Агента администрирования была выполнена не традиционным способом, с использованием дистрибутива, а, например, путем восстановления из образа диска.

- `-virtserv` – имя виртуального Сервера администрирования.

- `-cloningmode` – режим клонирования диска Агента администрирования.

  Используйте один из следующих параметров для настройки режима клонирования диска:

  - `-cloningmode` – запрос состояния режима клонирования диска.
  - `-cloningmode 1` – включить режим клонирования диска.
  - `-cloningmode 0` – выключить режим клонирования диска.

Например, чтобы подключить Агент администрирования к Серверу администрирования, выполните следующую команду:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

## Туннелирование соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом

устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

В частности, туннелирование используется для подключения к удаленному рабочему столу: как для подключения к существующей сессии, так и для создания новой удаленной сессии.

Также туннелирование может быть использовано при помощи механизма внешних инструментов. В частности, администратор может запускать таким образом утилиту putty, VNC-клиент и прочие инструменты.

Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

- Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
- Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт брандмауэром.

► *Чтобы произвести туннелирование соединения клиентского устройства с Сервером администрирования:*

1. В дереве консоли выберите папку группы, в которую входит клиентское устройство.
2. На закладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.
4. Создайте туннель в открывшемся окне **Туннелирование соединения**.

## Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве.

Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа. После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять программами, установленными на нем.

В этом разделе описывается, как установить соединение с клиентским устройством Windows (см. стр 717) и клиентским устройством macOS (см. стр. 719) с помощью Агента администрирования.

### См. также:



### Подключение к клиентским устройствам Windows

Удаленное подключение к клиентскому устройству с операционной системой Windows можно осуществить

одним из следующих способов:

- С помощью стандартного компонента Microsoft Windows "Подключение к удаленному рабочему столу".

  Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

- С помощью технологии совместного доступа к рабочему столу Windows.

**Подключение к клиентскому устройству Windows с помощью подключения к удаленному рабочему столу**

Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью компонента "Подключение к удаленному рабочему столу":*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи → Подключиться к устройству → Создать новую сессию RDP**.

   В результате будет запущена штатная утилита Windows mstsc.exe для подключения к удаленному рабочему столу.
3. Следуйте указаниям в открывающихся окнах утилиты.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

**Подключение к клиентскому устройству Windows с помощью совместного доступа к рабочему столу Windows**

При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита программа сохраняет информацию о файлах на устройстве, которые открывал и/или изменял администратор (см. стр. 721).

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в реестр Windows.

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky Security Center использует лицензию на Системное администрирование.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Подключиться к устройству** → **Совместный доступ к рабочему столу Windows**.
3. В открывшемся окне **Выбор сессии рабочего стола** выберите сеанс на клиентском устройстве, к которому требуется подключиться.

   В случае успешного подключения к клиентскому устройству рабочий стол этого устройства будет доступен в окне **Kaspersky Remote Desktop Session Viewer**.
4. Для начала взаимодействия с устройством в главном меню окна **Kaspersky Remote Desktop Session Viewer** выберите пункт **Действия** → **Интерактивный режим**.

## Подключение к клиентским устройствам macOS

Администратор может использовать систему Virtual Network Computing (VNC) для подключения к устройствам macOS.

Подключение к удаленному рабочему столу осуществляется через клиент VNC, установленный на устройстве Сервера администрирования. Клиент VNC переключает управление клавиатурой и мышью с клиентского устройства на администратора.

Когда администратор подключается к удаленному рабочему столу, пользователь не получает уведомлений или запросов на подключение от администратора. Администратор подключается к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе.

Для подключения к рабочему столу клиентского устройства Windows с помощью VNC клиента требуется выполнение следующих условий:

- Клиент VNC установлен на устройстве Сервера администрирования.
- На клиентском устройстве разрешены удаленный вход и удаленное управление.
- Пользователь разрешил администратору доступ к клиентскому устройству в свойствах **Общий доступ** операционной системы macOS.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью системы Virtual Network Computing (VNC):*

1. В дереве консоли администрирования выберите устройство, к которому требуется получить доступ.
2. В контекстном меню устройства выберите пункт **Все задачи** → **Туннелирование соединения**.

3. В открывшемся окне **Туннелирование соединения** выполните следующее:
   a. В разделе **Сетевой порт** укажите номер сетевого порта устройства, к которому вы хотите подключиться.

      По умолчанию номер порта – 5900.

   b. В разделе **Туннелирование** нажмите на кнопку **Создать туннель**.
   c. В разделе **Сетевые атрибуты** нажмите на кнопку **Копировать**.
4. Откройте клиент VNC и вставьте скопированные сетевые атрибуты в текстовое поле. Нажмите на клавишу **ENTER**.
5. В появившемся окне просмотрите параметры сертификата. Если вы согласны использовать сертификат, нажмите кнопку **Да**.
6. В окне **Аутентификация** укажите учетные данные клиентского устройства и нажмите на кнопку **ОК**.

## Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

► *Чтобы подключиться к устройству с помощью совместного доступа к рабочему столу Windows:*

1. В дереве консоли выберите папку **Управляемые устройства** на закладке **Устройства**.

   В рабочей области папки отображается список устройств.
2. В контекстном меню устройства, к которому вы хотите подключиться, выберите пункт **Подключиться к устройству → Совместный доступ к рабочему столу Windows**.

   Откроется окно **Выбор сессии рабочего стола**.
3. В окне **Выбор сессии рабочего стола** выберите сессию рабочего стола, которая будет использоваться для подключения к устройству.
4. Нажмите на кнопку **ОК**.

Будет выполнено подключение к устройству.

## Настройка перезагрузки клиентского устройства

В ходе работы, установки или удаления Kaspersky Security Center может потребоваться перезагрузка клиентского устройства. Вы можете настроить параметры перезагрузки только для устройств под управлением Windows.

► *Чтобы настроить перезагрузку клиентского устройства:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить перезагрузку.
2. В рабочей области группы выберите закладку **Политики**.
3. В списке политик выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Управление перезагрузкой**.
5. Выберите действие, которое нужно выполнять, если потребуется перезагрузка устройства:

- Выберите **Не перезагружать операционную систему**, чтобы запретить автоматическую перезагрузку.
- Выберите **При необходимости перезагрузить операционную систему автоматически**, чтобы разрешить автоматическую перезагрузку.
- Выберите **Запрашивать у пользователя**, чтобы включить запрос на перезагрузку у пользователя.

Вы можете указать периодичность запроса на перезагрузку, включить принудительную перезагрузку и принудительное закрытие программ в заблокированных сессиях на устройстве, установив соответствующие флажки и интервалы.

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате перезагрузка операционной системы устройства будет настроена.

## Аудит действий на удаленном клиентском устройстве

Программа позволяет выполнять аудит действий администратора на удаленных клиентских устройствах под управлением Windows. В ходе аудита программа сохраняет информацию о файлах на устройстве, которые открывал и / или изменял администратор. Аудит действий администратора доступен при выполнении следующих условий:

- лицензия на Системное администрирование уже используется;
- у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

► *Чтобы включить аудит действий на удаленном клиентском устройстве:*

1. В дереве консоли выберите группу администрирования, для которой нужно настроить аудит действий администратора.
2. В рабочей области группы выберите закладку **Политики**.
3. Выберите политику Агента администрирования Kaspersky Security Center и в контекстном меню политики выберите пункт **Свойства**.
4. В окне свойств политики выберите раздел **Совместный доступ к рабочему столу Windows**.
5. Установите флажок **Включить аудит**.
6. В списках **Маски файлов, чтение которых нужно отслеживать** и **Маски файлов, изменение которых нужно отслеживать** добавьте маски файлов, действия с которыми нужно отслеживать в ходе аудита.

   По умолчанию программа отслеживает действия с файлами с расширениями .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt и .pdf.
7. Нажмите на кнопку **ОК**, чтобы сохранить изменения и закрыть окно свойств политики.

В результате аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу будет настроен.

Записи о действиях администратора на удаленном устройстве сохраняются:

- в журнале событий на удаленном устройстве;
- в файле с расширением syslog, который находится в папке Агента администрирования на удаленном устройстве (например, C:\ProgramData\KasperskyLab\adminkit\1103\logs);
- в базе событий Kaspersky Security Center.

kaspersky

## Проверка соединения клиентского устройства с Сервером администрирования

Kaspersky Security Center позволяет проверять соединение клиентского устройства с Сервером администрирования автоматически или вручную.

Автоматическая проверка соединения осуществляется на Сервере администрирования. Проверка соединения вручную осуществляется на устройстве.

### В этом разделе



### Автоматическая проверка соединения клиентского устройства с Сервером администрирования

► *Чтобы запустить автоматическую проверку соединения клиентского устройства с Сервером администрирования:*

1. В дереве консоли выберите группу администрирования, в которую входит устройство.
2. В рабочей области группы администрирования на закладке **Устройства** выберите устройство.
3. В контекстном меню устройства выберите пункт **Проверить доступность устройства**.

В результате открывается окно, содержащее информацию о доступности устройства.

### Проверка соединения клиентского устройства с Сервером администрирования вручную. Утилита klnagchk

Вы можете проверять соединение и получать подробную информацию о параметрах подключения клиентского устройства к Серверу администрирования с помощью утилиты klnagchk.

При установке на устройство Агента администрирования утилита klnagchk автоматически копируется в папку установки Агента администрирования.

При запуске из командной строки утилита klnagchk в зависимости от используемых ключей выполняет следующие действия:

- Выводит на экран или заносит в файл журнала событий значения параметров подключения Агента администрирования, установленного на устройстве, к Серверу администрирования.
- Записывает в файл журнала событий статистику Агента администрирования (с момента его последнего запуска) и результаты выполнения утилиты, либо выводит информацию на экран.
- Предпринимает попытку установить соединение Агента администрирования с Сервером администрирования.

  Если соединение установить не удалось, утилита посылает ICMP-пакет для проверки статуса устройства, на котором установлен Сервер администрирования.

► *Чтобы проверить соединение клиентского устройства с Сервером администрирования с помощью утилиты klnagchk,*

на устройстве запустите утилиту klnagchk из командной строки.

Синтаксис командной строки утилиты:

```
klnagchk [-logfile <имя файла>] [-sp] [-savecert <путь к файлу сертификата>] [-restart]
```

Описания ключей:

- `-logfile <имя файла>` – записать значения параметров подключения Агента администрирования к Серверу и результаты выполнения утилиты в файл журнала.

  По умолчанию информация сохраняется в стандартном потоке вывода (stdout). Если ключ не используется, параметры, результаты и сообщения об ошибках выводятся на экран.

- `-sp` – вывести пароль для аутентификации пользователя на прокси-сервере.

  Параметр используется, если подключение к Серверу администрирования осуществляется через прокси-сервер.

- `-savecert <имя файла>` – сохранить сертификат для аутентификации доступа к Серверу администрирования в указанном файле.

- `-restart` – перезапустить Агент администрирования после завершения работы утилиты.

### О проверке времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Консоли администрирования такое устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Время последнего подключения** (значение атрибута отображается в Консоли администрирования в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

## Идентификация клиентских устройств на Сервере администрирования

Идентификация клиентских устройств осуществляется на основании их имен. Имя устройства является уникальным среди всех имен устройств, подключенных к Серверу администрирования.

Имя устройства передается на Сервер администрирования либо при опросе сети Windows и обнаружении в ней нового устройства, либо при первом подключении к Серверу администрирования установленного на устройстве Агента администрирования. По умолчанию имя совпадает с именем устройства в сети Windows (NetBIOS-имя). Если на Сервере администрирования уже зарегистрировано устройство с таким именем, то к имени нового устройства будет добавлено окончание с порядковым номером, например: **<Имя>-1**, **<Имя>-2**. Под этим именем устройство включается в состав группы администрирования.

## Перемещение устройств в состав группы администрирования

Устройства можно перемещать из одной группы администрирования в другую только при наличии прав (см. стр. 798) **Изменение** в области **Управление группами администрирования** как для исходных, так и для целевых групп администрирования (или для Сервера администрирования, к которым принадлежат эти группы).

► *Чтобы включить одно или несколько устройств в состав выбранной группы администрирования:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В папке **Управляемые устройства** выберите вложенную папку, соответствующую группе, в состав которой будут включены клиентские устройства.

   Если вы хотите включить устройства в состав группы **Управляемые устройства**, этот шаг можно пропустить.
3. В рабочей области выбранной группы администрирования на закладке **Устройства** запустите процесс включения устройств в группу одним из следующих способов:
   - Добавьте устройства в группу по кнопке **Переместить устройства в группу** в блоке работы со списком устройств.
   - В контекстном меню списка устройств выберите **Создать** → **Устройство**.

   В результате запустится мастер перемещения устройств. Следуя его указаниям, определите способ перемещения устройств в группу и сформируйте список устройств, включаемых в состав группы.

   Если вы формируете список устройств вручную, в качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя. Вручную в список устройств могут быть перемещены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Для импорта списка устройств из файла требуется указать файл в формате TXT с перечнем адресов добавляемых устройств. Каждый адрес должен располагаться в отдельной строке.

После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

Можно переместить устройство в выбранную группу администрирования, перетащив его мышью из папки **Нераспределенные** устройства в папку группы администрирования.

## Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи *Смена Сервера администрирования*.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу смены Сервера администрирования одним из следующих способов:

- Если требуется сменить Сервер администрирования для устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. стр. 413).
- Если требуется сменить Сервер администрирования для устройств, входящих в разные группы администрирования или не входящих в группы администрирования, создайте задачу для набора устройств (см. стр. 415).

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу *Смена Сервера администрирования*.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Если Сервер администрирования поддерживает управление шифрованием и защитой данных, то при создании задачи *Смена Сервера администрирования* отображается предупреждение. Предупреждение содержит информацию о том, что при наличии на устройствах зашифрованных данных после переключения устройств под управлением другого Сервера пользователям будет предоставлен доступ только к тем зашифрованным данным, с которыми они работали ранее. В остальных случаях доступ к зашифрованным данным предоставлен не будет. Подробное описание сценариев, в которых доступ к зашифрованным данным не будет предоставлен, приведено в онлайн-справке Kaspersky Endpoint Security для Windowshttps://support.kaspersky.com/help/KESWin/11.5.0/ru-RU/128089.htm.

## Кластеры и массивы серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что программа, установленная на клиентском устройстве, является частью массива сервера, то клиентское устройство становится узлом кластера. Кластер будет добавлен как отдельный объект в папке **Управляемые устройства** в дереве консоли со значком  .

Можно выделить несколько типичных свойств кластера:

- Кластер и любой из его узлов всегда располагаются в одной группе администрирования.
- Если администратор попытается переместить какой-либо узел кластера, то узел вернется в исходное местоположение.
- Если администратор попытается переместить кластер в другую группу, то все его узлы также переместятся вместе с ним.

## Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

► *Чтобы удаленно управлять клиентскими устройствами:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу управления устройствами одним из следующих способов:

- Если требуется включить, выключить или перезагрузить устройства, входящие в выбранную группу администрирования, создайте задачу для выбранной группы (см. стр. 413).
- Если требуется включить, выключить или перезагрузить устройства, входящие в разные группы администрирования или не входящие в группы администрирования, создайте задачу для набора устройств (см. стр. 415).

Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне **Тип задачи** мастера создания задачи выберите узел **Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Управление устройствами**.

3. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

## Об использовании постоянного соединения между управляемым устройством и Сервером администрирования

По умолчанию в Kaspersky Security Center нет постоянных соединений между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Интервал между этими сеансами синхронизации определяется в политике Агента администрирования и по умолчанию составляет 15 минут. Если необходима досрочная синхронизация (например, для ускорения применения политики), то Сервер администрирования посылает Агенту администрирования подписанный сетевой пакет на порт UDP 15000. Сервер администрирования может отправить этот пакет по IPv4-сети или IPv6-сети. Если подключение по UDP от Сервера администрирования к управляемому устройству по какой-то причине невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Однако некоторые операции невозможно выполнить без подключения Агента администрирования к Серверу администрирования. Эти операции включают запуск и остановку локальных задач, получение статистики для управляемой программы и создание туннеля. Чтобы сделать эти операции возможными, включите параметр **Не разрывать соединение с Сервером администрирования** на управляемом устройстве (см. стр.742).

### См. также:

Информация об ограничениях Kaspersky Security Center.....170

## О принудительной синхронизации

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

В контекстном меню управляемых устройств в Консоли администрирования в пункте меню **Все задачи** имеется команда **Синхронизировать принудительно**. Когда Kaspersky Security Center 12 выполняет эту команду, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

### См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

## О расписании соединений

В окне свойств политики Агента администрирования в разделе **Подключения** во вложенном разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования.

**Подключаться при необходимости**. Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

**Подключаться в указанные периоды**. Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

## Отправка сообщения пользователям устройств

► *Чтобы отправить сообщение пользователям устройств:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Создайте задачу отправки сообщения пользователям устройств одним из следующих способов:
   - Если требуется отправить сообщение пользователям устройств, входящих в выбранную группу администрирования, создайте задачу для выбранной группы (см. стр. 413).
   - Если требуется отправить сообщение пользователям устройств, входящих в разные группы администрирования или не принадлежащих ни одной группе администрирования, создайте задачу для набора устройств (см. стр. 415).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. В окне Тип задачи мастера создания задачи выберите узел **Сервер администрирования Kaspersky Security Center**, раскройте папку **Дополнительно** и выберите задачу **Сообщение для пользователя**. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными записями пользователей** (см. 801).
4. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Отправка сообщений пользователю с помощью задачи доступна только для устройств под управлением операционной системы Windows. Также вы можете отправить сообщение из контекстного меню пользователя из рабочей области папки **Управление учетными записями пользователей** (см. 801).

## Работа с программой Kaspersky Security для виртуальных сред

Kaspersky Security Center поддерживает возможность подключения виртуальных машин к Серверу администрирования. Защита виртуальных машин осуществляется с помощью программы Kaspersky Security для виртуальных сред. Подробнее см. в документации к этой программе.

## Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► *Чтобы изменить статус устройства на* Критический*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Критический"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

► *Чтобы изменить статус устройства на* Предупреждение*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Предупреждение"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением `Более 7 дней` клиентскому устройству присваивается статус *Предупреждение*, а со значением `Более 14 дней` – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

*Таблица 67. Условия присвоения статусов устройству*

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Не установлена программа безопасности | Агент администрирования установлен на устройстве, но не установлена программа безопасности. | • Флажок установлен.<br>• Флажок снят. |
| Обнаружено много вирусов | В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение. | Более 0 |

| Условие | Описание условия | Доступные значения |
| --- | --- | --- |
| Уровень постоянной защиты отличается от уровня, установленного администратором | Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства. | • Остановлена.<br>• Приостановлена.<br>• Выполняется. |
| Давно не выполнялся поиск вредоносного ПО | Устройство видимо в сети и на устройстве установлена программа безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее. | Более 1 дня |
| Базы устарели | Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее. | Более 1 дня |
| Давно не подключался | Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. | Более 1 дня |
| Есть активные угрозы | Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение. | Более чем 0 штук |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Требуется перезагрузка | Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин. | Более чем 0 минут |
| Установлены несовместимые программы | Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы. | • Флажок снят.<br>• Флажок установлен. |
| Обнаружены уязвимости в программах | Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в программах с заданным уровнем критичности. | • Предельный.<br>• Высокий.<br>• Средний.<br>• Игнорировать, если нельзя закрыть уязвимость.<br>• Игнорировать, если обновление назначено к установке. |
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истек. | • Флажок снят.<br>• Флажок установлен. |
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней. | Более чем 0 дней |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Давно не выполнялась проверка обновлений Центра обновления Windows | Не выполнялась задача Синхронизация обновлений Windows Update больше указанного времени. | Более 1 дня |
| Указанный статус шифрования | Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению. | • Не соответствует политике из-за отказа пользователя (только для внешних устройств).<br>• Не соответствует политике из-за ошибки.<br>• В процессе применения политики – требуется перезагрузка.<br>• Не задана политика шифрования.<br>• Не поддерживается.<br>• В процессе применения политики. |
| Параметры мобильного устройства не соответствуют политике | Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия. | • Флажок снят.<br>• Флажок установлен. |
| Есть необработанные инциденты | На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. | • Флажок снят.<br>• Флажок установлен. |
| Статус устройства определен программой | Статус устройства определяется управляемой программой. | • Флажок снят.<br>• Флажок установлен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| На устройстве заканчивается дисковое пространство | Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению. | Более чем 0 МБ |
| Устройство стало неуправляемым | Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования. | • Флажок снят.<br>• Флажок установлен. |
| Защита выключена | Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени. | Более чем 0 минут |
| Программа безопасности не запущена | Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена. | • Флажок снят.<br>• Флажок установлен. |

См. также:

Настройка общих параметров Сервера администрирования .....685

## Назначение тегов устройствам и просмотр назначенных тегов

Kaspersky Security Center позволяет назначать теги устройствам. *Тег* представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Ручное назначение тегов устройству выполняется в свойствах устройства и может понадобиться, когда необходимо отметить отдельное устройство. Автоматическое назначение тегов выполняется Сервером администрирования в соответствии с заданными правилами назначения тегов.

В свойствах Сервера администрирования вы можете настроить автоматическое назначение тегов устройствам, управляемым этим Сервером администрирования. Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное

правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве программам и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы Windows, назначается тег *Win*. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать устройства, работающие под управлением операционной системы Windows, и назначить им задачу.

Вы также можете использовать теги в качестве условия для активации профиля политики на управляемом устройстве, чтобы определенные профили политик применялись только на устройствах, имеющих определенные теги. Например, если в группе администрирования *Пользователи* появляется устройство с тегом *Курьер* и по тегу *Курьер* настроена активация соответствующего профиля политики, то к этому устройству будет применяться не сама политика, созданная для группы *Пользователи*, а ее профиль. Профиль политики может разрешить на этом устройстве запуск отдельных программ, которые запрещено запускать в рамках политики.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов в свойствах устройства. Каждое правило назначения тегов можно включить или выключить. Если правило включено, оно применяется к устройствам, управляемым Сервером администрирования. Если правило не нужно, но может понадобиться в дальнейшем, то нет необходимости его удалять; достаточно снять флажок **Включить правило**. При этом правило выключается и не выполняется до тех пор, пока флажок **Включить правило** не будет установлен. Отключение правила без удаления может потребоваться, если это правило необходимо временно исключить из списка правил назначения тегов, а потом опять включить.

## В этом разделе



## Автоматическое назначение тегов устройствам

Вы можете создавать и изменять правила автоматического назначения тегов в окне свойств Сервера администрирования.

► *Чтобы автоматически назначить теги устройствам:*

1. В дереве консоли выберите узел с именем Сервера администрирования, для которого требуется задать правила назначения тегов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Правила назначения тегов**.
4. Выберите раздел **Правила назначения тегов** и нажмите на кнопку **Добавить**.

   Откроется окно **Новое правило**.
5. В окне **Новое правило** настройте общие свойства правила:
   - Укажите имя правила.

     Имя правила не может превышать 255 символов и содержать специальные символы (`"*<>?\:|`).
   - Включите или выключите правило с помощью флажка **Включить правило**.

     По умолчанию флажок **Включить правило** установлен.

- В поле **Тег** введите название тега.

  Название тега не может превышать 255 символов и содержать специальные символы ("*<>?\:|).

6. В разделе **Условия** нажмите на кнопку **Добавить**, чтобы добавить новое условие, или нажмите на кнопку **Свойства**, чтобы изменить существующее условие.

   Откроется окно мастера создания условия для правила автоматического назначения тегов.

7. В окне **Условия назначения тега** установите флажки для тех условий, которые должны влиять на назначения тега. Можно выбрать несколько условий.
8. В зависимости от того, какие условия назначения тега вы выбрали, мастер покажет окна для настройки соответствующих условий. Настройте срабатывание правила по следующим условиям:

   - **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену, к IP-диапазону).

     Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

   - **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
   - **Программы** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
   - **Виртуальные машины** – принадлежность устройства к разным типам виртуальных машин.
   - **Реестр программ** – наличие на устройстве программ различных производителей.

9. После настройки условия введите название условия и завершите работу мастера.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий. Добавленные условия отображаются в окне свойств правила.

10. Нажмите на кнопку **ОК** в окне **Новое правило** и на кнопку **ОК** в окне свойств Сервера администрирования.

Созданные правила выполняются на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

## Просмотр и настройка тегов, назначенных устройству

Вы можете просмотреть список всех тегов, назначенных устройству, а также перейти к настройке правил автоматического назначения тегов в окне свойств устройства.

► *Чтобы просмотреть и настроить назначенные устройству теги:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** выберите устройство, для которого вы хотите посмотреть назначенные теги.
3. В контекстном меню выбранного устройства выберите пункт **Свойства**.
4. В окне свойств устройства выберите раздел **Теги**.

Отобразится список тегов, назначенных выбранному устройству, а также способ назначения тега: вручную или по правилу.

5. При необходимости выполните одно из следующих действий:
   - Чтобы перейти к настройке правил назначения тегов, перейдите по ссылке **Настроить правила автоматического назначения тегов** (только для устройств с операционной системой Windows).
   - Чтобы переименовать тег, выделите тег и нажмите на кнопку **Переименовать**.
   - Чтобы удалить тег, выделите тег и нажмите на кнопку **Удалить**.
   - Чтобы добавить тег вручную, введите тег в поле в нижней части раздела **Теги** и нажмите на кнопку **Добавить**.
6. Нажмите на кнопку **Применить**, если вы делали изменения в разделе **Теги**, чтобы ваши изменения вступили в силу.
7. Нажмите на кнопку **ОК**.

Если вы удалили или переименовали тег в свойствах устройства, это изменение не распространится на правила назначения тегов, заданные в свойствах Сервера администрирования. Изменение будет применено только к тому устройству, в свойства которого вы внесли изменение.

## Удаленная диагностика клиентских устройств. Утилита удаленной диагностики Kaspersky Security Center

Утилита удаленной диагностики Kaspersky Security Center (далее – утилита удаленной диагностики) предназначена для удаленного выполнения на клиентских устройствах следующих операций:

- включения и выключения трассировки, изменения уровня трассировки, загрузки файла трассировки;
- загрузки системной информации и параметров программы;
- загрузки журналов событий;
- создание файла дампа для программы;
- запуска диагностики и загрузки результатов диагностики;
- запуска и остановки программ.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также специалист Службы технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Утилита удаленной диагностики автоматически устанавливается на устройство совместно с Консолью администрирования.

kaspersky

## В этом разделе



## Подключение утилиты удаленной диагностики к клиентскому устройству

► *Чтобы подключить утилиту удаленной диагностики к клиентскому устройству:*

1. В дереве консоли выберите любую группу администрирования.
2. В рабочей области на закладке **Устройства** в контекстном меню любого устройства выберите пункт **Внешние инструменты → Удаленная диагностика**.

   В результате открывается главное окно утилиты удаленной диагностики.
3. В первом поле главного окна утилиты удаленной диагностики определите, какими средствами требуется подключиться к устройству:
   - **Доступ средствами сети Microsoft Windows**.
   - **Доступ средствами Сервера администрирования**.
4. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами сети Microsoft Windows**, выполните следующие действия:
   - В поле **Устройство** укажите адрес устройства, к которому требуется подключиться.

     В качестве адреса устройства можно использовать IP-адрес, NetBIOS- или DNS-имя.

     По умолчанию указан адрес устройства, из контекстного меню которого запущена утилита.
   - Укажите учетную запись для подключения к устройству:
     - **Подключиться от имени текущего пользователя** (выбрано по умолчанию). Подключитесь под учетной записью текущего пользователя.
     - **При подключении использовать предоставленное имя пользователя и пароль**. Подключитесь под указанной учетной записью. Укажите **Имя пользователя** и **Пароль** нужной учетной записи.

     Подключение к устройству возможно только под учетной записью локального администратора устройства.
5. Если в первом поле главного окна утилиты вы выбрали вариант **Доступ средствами Сервера администрирования**, выполните следующие действия:
   - В поле **Сервер администрирования** укажите адрес Сервера администрирования, с которого следует подключиться к устройству.

В качестве адреса Сервера можно использовать IP-адрес, NetBIOS- или DNS-имя.

По умолчанию указан адрес Сервера, с которого запущена утилита.

- Если требуется, установите флажки **Использовать SSL**, **Сжимать трафик** и **Устройство принадлежит подчиненному Серверу администрирования**.

  Если установлен флажок **Устройство принадлежит подчиненному Серверу администрирования**, в поле **Подчиненный Сервер администрирования** вы можете выбрать подчиненный Сервер администрирования, под управлением которого находится устройство, нажав на кнопку **Обзор**.

6. Для подключения к устройству нажмите на кнопку **Войти**.

> Вы должны авторизовываться с помощью двухэтапной проверки (см. стр. 702), если двухэтапная проверка для вашей учетной записи включена.

В результате откроется окно удаленной диагностики устройства (см. рис. ниже). В левой части окна расположены ссылки для выполнения операций по диагностике устройства. В правой части окна расположено дерево объектов устройства, с которыми может работать утилита. В нижней части окна отображается процесс выполнения операций утилиты.

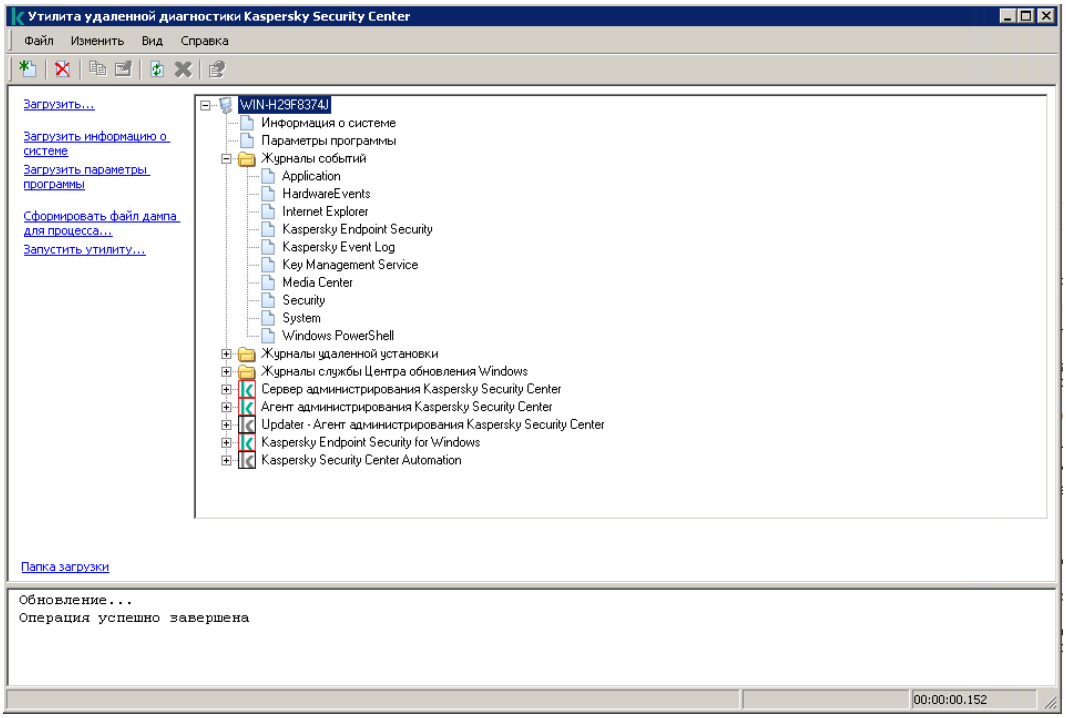



Figure 5. Утилита удаленной диагностики. Окно удаленной диагностики клиентского компьютера

> Утилита удаленной диагностики сохраняет загруженные с устройств файлы на рабочем столе устройства, с которого она запущена.

## См. также:

## Включение и выключение трассировки, загрузка файла трассировки

► *Чтобы включить трассировку на удаленном устройстве:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству (на стр. 736).
2. В дереве объектов устройства выберите программу, для которой требуется включить трассировку.

   Включение и выключение трассировки у программ с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

   Если вы хотите включить трассировку для Агента администрирования, вы также можете сделать это при создании задачи Установка требуемых обновлений и закрытие уязвимостей (на стр. 527). В этом случае Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики.
3. Чтобы включить трассировку:
   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку**.
   b. В открывшемся окне **Выбор уровня трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:
      - **Уровень трассировки**

Уровень трассировки определяет состав информации, которую содержит файл трассировки.

      - **Трассировка на основе ротации** (доступно только для Kaspersky Endpoint Security)

Программа перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

   a. Нажмите на кнопку **ОК**.

1. Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

   Чтобы включить трассировку xperf:

   a. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Включить трассировку Xperf**.
   b. В открывшемся окне **Выбор уровня трассировки**, в зависимости от запроса специалиста Службы технической поддержки, выберите один из следующих уровней трассировки:
      - **Легкий уровень**

        Файл трассировки этого типа содержит минимальный объем информации о системе.

        По умолчанию выбран этот вариант.

      - **Детальный уровень**

        Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Службы технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит

информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и программ, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

c. Выберите один из уровней трассировки:

- **Базовый тип**

  Программа получает данные трассировки во время работы программы Kaspersky Endpoint Security.

  По умолчанию выбран этот вариант.

- **Тип перезагрузки**

  Программа получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

d. Также вам могут предложить включить параметр **Трассировка на основе ротации**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

e. Нажмите на кнопку **ОК**.

В некоторых случаях для включения трассировки программы безопасности требуется перезапустить эту программу и ее задачу.

Утилита удаленной диагностики позволяет получать трассировку для выбранной программы.

► *Чтобы загрузить файл трассировки программы:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В узле программы в папке **Файлы трассировки** выберите требуемый файл.
3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить файл**.

   Для файлов большого объема есть возможность загрузить только последние части трассировки.

   Вы можете удалить выделенный файл трассировки. Удаление файла возможно после выключения трассировки.

Выбранный файл загружается в местоположение, указанное в нижней части окна.

► *Чтобы выключить трассировку на удаленном устройстве:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В дереве объектов устройства выберите программу, для которой требуется выключить трассировку.

   Включение и выключение трассировки у программ с самозащитой возможно только при подключении к устройству средствами Сервера администрирования.

3. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Выключить трассировку**.

Утилита удаленной диагностики выключит трассировку для выбранной программы.

## Загрузка параметров программ

► *Чтобы загрузить с удаленного устройства параметры программ:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В дереве объектов окна утилиты удаленной диагностики выберите верхний узел с именем устройства.
3. В левой части окна утилиты удаленной диагностики выберите требуемое действие из следующих параметров:
   - **Загрузить информацию о системе**
   - **Загрузить параметры программы**
   - **Сформировать файл дампа для процесса.**

     В окне, открывшемся по этой ссылке, укажите исполняемый файл программы, для которого нужно сформировать файл дампа.
   - **Запустить утилиту**

     В окне, открывшемся по этой ссылке, укажите исполняемый файл утилиты, которую вы хотите запустить, и параметры ее запуска.

В результате выбранная утилита будет загружена на устройство и запущена на нем.

## Загрузка журналов событий

► *Чтобы загрузить с удаленного устройства журнал событий:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В папке **Журнал событий** в дереве объектов устройства выберите соответствующий журнал событий.
3. Чтобы загрузить журнал событий, перейдите по ссылке **Загрузить журнал событий <Имя журнала событий>** в левой части окна утилиты удаленной диагностики.

Выбранный журнал событий загружается в местоположение, указанное в нижней части окна.

## Загрузка нескольких диагностических информационных элементов

Утилита удаленной диагностики Kaspersky Security Center позволяет загружать несколько элементов диагностической информации, включая журналы событий, системную информацию, файлы трассировки и файлы дампа.

► *Чтобы загрузить с удаленного устройства диагностическую информацию:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В левой части окна утилиты удаленной диагностики нажмите на кнопку **Загрузить**.
3. Установите флажки напротив объектов, которые вы хотите загрузить.
4. Нажмите на кнопку **Запустить**.

Каждый выбранный объект загружается в месторасположение, указанное в нижней панели.

## Запуск диагностики и загрузка ее результатов

► *Чтобы запустить диагностику программы на удаленном устройстве и загрузить ее результаты:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В дереве объектов устройства выберите необходимую программу.
3. Чтобы запустить диагностику, перейдите по ссылке **Выполнить диагностику** в левой части окна утилиты удаленной диагностики.

   В результате в узле выбранной программы в дереве объектов появится отчет диагностики.
4. Выберите сформированный отчет диагностики в дереве объектов и скачайте его по ссылке **Загрузить файл**.

Выбранный отчет загружается в местоположение, указанное в нижней части окна.

## Запуск, остановка и перезапуск программ

Запуск, остановка и перезапуск программ возможны только при подключении к устройству средствами Сервера администрирования.

► *Чтобы запустить, остановить или перезапустить программу:*

1. Запустите утилиту удаленной диагностики и подключитесь к нужному вам устройству, как описано в разделе "Подключение утилиты удаленной диагностики к клиентскому устройству (на стр. 736)".
2. В дереве объектов устройства выберите необходимую программу.
3. Выберите действие в левой части окна утилиты удаленной диагностики:
   - **Остановить программу.**
   - **Перезапустить программу.**
   - **Запустить программу.**

В зависимости от выбранного вами действия программа запустится, остановится или перезапустится.

## Устройства с защитой на уровне UEFI

*Устройство с защитой на уровне UEFI* – это устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

► *Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования выберите раздел **Параметры подключения к Серверу → Дополнительные порты**.
4. В разделе **Дополнительные порты** измените необходимые вам параметры:
   - **Открыть порт для устройств с защитой на уровне UEFI**

     Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

   - **Порт для устройств с защитой на уровне UEFI**

     Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI**. По умолчанию установлен порт 13294.
5. Нажмите на кнопку **ОК**.

## Параметры управляемого устройства

► *Чтобы просмотреть параметры управляемого устройства:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки выберите устройство.
3. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.

Откроется окно свойств устройства с выбранным разделом **Общие**.

Общие

Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:

- **Имя**

  В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

- **Описание**

  В поле можно ввести дополнительное описание клиентского устройства.

- **Windows-домен**

  Windows-домен или рабочая группа, в которую входит устройство.

- **NetBIOS-имя**

  Имя клиентского устройства в сети Windows.

- **DNS-имя**

  Имя DNS-домена клиентского устройства.

- **IP-адрес**

  IP-адрес устройства.

- **Группа**

  Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление**

  Дата последнего обновления антивирусных баз или программ на устройстве.

- **Последнее появление в сети**

  Дата и время, когда устройство последний раз было видимо в сети.

- **Соединение с Сервером**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

  Если этот параметр включен, сохраняется постоянное соединение между управляемым устройством и Сервером администрирования. Вы можете использовать этот параметр, если не используете push-серверы (см. стр. 668), которые обеспечивают такое соединение.

  Если параметр выключен и push-серверы не используются, управляемое устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  Общее количество устройств с выбранным параметром **Не разрывать соединение с Сервером администрирования** не может превышать 300.

  Этот параметр по умолчанию выключен на управляемых устройствах. Этот параметр включен по умолчанию на устройстве, на котором установлен Сервер администрирования, и остается включенным, даже если вы попытаетесь его выключить.

Защита

В разделе **Защита** представлена информация о состоянии антивирусной защиты на клиентском устройстве:

- **Статус устройства**

  Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

- **Все проблемы**

  Эта таблица содержит полный список проблем, обнаруженных управляемыми программами, установленными на клиентском устройстве. Каждая проблема имеет статус, который управляемая программа предлагает вам назначить устройству из-за этой проблемы.

- **Статус постоянной защиты**

  Статус текущего состояния постоянной защиты (на странице 899) клиентского устройства.

  После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.

- **Последняя проверка по требованию**

  Дата и время последнего поиска вредоносного ПО на клиентском устройстве.

- **Всего обнаружено угроз**

Общее количество обнаруженных на клиентском устройстве угроз с момента установки программы безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- **Активные угрозы**

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

- **Статус шифрования дисков**

  Текущее состояние шифрования файлов на локальных дисках устройства. Описание статусов см. в онлайн-справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/65058.htm.

Программы

В разделе **Программы** отображается список программ "Лаборатории Касперского", установленных на клиентском устройстве.

- **События**

  При нажатии на кнопку можно просмотреть список событий, произошедших на клиентском устройстве при работе программы, а также результаты выполнения задач для этой программы.

- **Статистика**

  При нажатии на кнопку можно просмотреть текущую статистическую информацию о работе программы.

- **Свойства**

  При нажатии на кнопку можно получить информацию о программе и выполнить настройку программы.

Задачи

На закладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. В случае отсутствия связи статус не отображается.

События

На закладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

Теги

На закладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

Информация о системе

В разделе **Общая информация о системе** представлена информация о программе, установленной на клиентском устройстве.

Реестр программ

В разделе **Реестр программ** можно просмотреть реестр установленных на клиентском устройстве программ и обновлений для них, а также настроить отображение реестра программ.

Информация об установленных программах предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**. Информация об установленных программах доступна только для устройств под управлением Windows.

Агент администрирования предоставляет информацию о программах на основе данных системного реестра.

- **Показывать только несовместимые программы безопасности**

  Если параметр включен, в списке программ отображаются только те программы безопасности, которые несовместимы с программами "Лаборатории Касперского".

  По умолчанию параметр выключен.

- **Показывать обновления**

  Если параметр включен, в списке программ отображаются не только программы, но и установленные для них пакеты обновлений.

  Для отображения списка обновлений необходимо 100 КБ трафика. Если вы закроете список и снова откроете его, вам снова придется потратить 100 КБ трафика.

  По умолчанию параметр выключен.

- **Экспортировать в файл**

Нажмите эту кнопку, чтобы экспортировать список программ, установленных на устройстве, в файл формата CSV или TXT.

- **История**

Нажмите эту кнопку, чтобы просмотреть события, относящиеся к установке программ на устройство. Отобразится следующая информация:

- дата и время, когда программа была установлена на устройство;
- название программы;
- версия программы.

- **Свойства**

Нажмите эту кнопку, чтобы просмотреть свойства программы, выбранной в списке программ, установленных на устройстве. Отобразится следующая информация:

- название программы;
- версия программы;
- поставщик программы.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

Реестр оборудования

В разделе **Реестр оборудования** можно просмотреть информацию об оборудовании, установленном на клиентском устройстве. Эту информацию можно просматривать для устройств я операционными системами Windows и Linux.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить сведения об оборудовании. Сведения об оборудовании, полученные от виртуальных машин, могут быть неполными в зависимости от используемого гипервизора.

Сеансы

В разделе **Сеансы** представлена информация о владельце клиентского устройства, а также об учетных записях пользователей, которые работали с выбранным клиентским устройством.

Информация о доменных пользователях формируется на основе данных Active Directory. Информация о локальных пользователях предоставляется Диспетчером учетных записей безопасности (Security Account Manager), установленным на клиентском устройстве.

- **Владелец устройства**

В поле **Владелец устройства** отображается имя пользователя, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с клиентским устройством.

По кнопкам **Назначить** и **Свойства** можно выбрать владельца устройства и просмотреть информацию о пользователе, назначенном владельцем устройства.

По кнопке с красным крестом можно удалить текущего владельца устройства.

В списке содержатся учетные записи пользователей, которые работают с клиентским устройством.

- **Имя**

  Имя устройства в Windows-сети.

- **Имя участника**

  Имя пользователя (доменное или локальное), который выполнил вход в систему на этом устройстве.

- **Учетная запись**

  Учетная запись пользователя, который выполнил вход в систему на этом устройстве.

- **Электронная почта**

  Адреса электронной почты пользователя.

- **Номер телефона**

  Номер телефона пользователя.

Инциденты

На закладке **Инциденты** можно просматривать, редактировать и создавать инциденты для клиентского устройства. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. Например,

если пользователь постоянно переносит на устройство вредоносные программы с личного съемного диска, администратор может создать инцидент. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте инцидента, и может добавить ссылку на пользователя или пользователей.

Инцидент, для которого выполнены необходимые действия, называется *обработанным*. Наличие необработанных инцидентов может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список инцидентов, созданных для устройства. Инциденты классифицируются по уровню важности и типу. Тип инцидента определяется программой "Лаборатории Касперского", которая создает инцидент. Обработанные инциденты можно отметить в списке, установив флажок в графе **Обработан**.

Уязвимости в программах

В разделе **Уязвимости в программах** можно просмотреть список с информацией об уязвимостях сторонних программ, установленных на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке уязвимости по имени уязвимости.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить список уязвимостей в файле. По умолчанию программа экспортирует список уязвимостей в файл формата CSV.

- **Показывать только те уязвимости, которые можно закрыть**

  Если параметр включен, в разделе отображаются уязвимости, которые можно закрыть патчем.

  Если параметр выключен, в разделе отображаются и уязвимости, которые можно закрыть патчем, и уязвимости, для которых патч отсутствует.

  По умолчанию параметр включен.

- **Свойства**

  Выберите уязвимость в программах в списке и нажмите на кнопку **Свойства**, чтобы просмотреть свойства выбранной уязвимости в программах в отдельном окне. В окне свойств можно выполнить следующие действия:

  - Пропустить уязвимость в программах на этом управляемом устройстве (в Консоли администрирования (на стр. 548) или в Kaspersky Security Center 14.2 Web Console (на стр. 742)).
  - Просмотреть список рекомендуемых исправлений для уязвимости.
  - Вручную указать обновления программного обеспечения для закрытия уязвимости (в Консоли администрирования (на странице 549) или в Kaspersky Security Center 14.2 Web Console (на стр. 1330)).
  - Просмотреть экземпляр уязвимости.
  - Просмотреть список существующих задач для закрытия уязвимости и создать задачи для закрытия уязвимости.

Неустановленные обновления

В этом разделе можно просмотреть список обнаруженных на устройстве обновлений программного обеспечения, которые не были установлены.

- **Показывать установленные обновления**

  Если параметр включен, в списке обновлений отображаются и не установленные обновления, и обновления, которые уже установлены на клиентском устройстве.

  По умолчанию параметр выключен.

Активные политики

В этом разделе отображается список политик для программ "Лаборатории Касперского", активных на устройстве в настоящее время.

- **Экспортировать в файл**

По кнопке **Экспортировать в файл** вы можете сохранить список активных политик в файле. По умолчанию программа экспортирует список политик в файл формата CSV.

Действующие профили политик

- **Действующие профили политик**

  В списке можно просмотреть информацию о действующих профилях политики, которые активны на клиентских устройствах. С помощью строки поиска над списком вы можете искать в списке действующие профили политик по имени политики или по имени профиля политики.

- **Экспортировать в файл**

Точки распространения

В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.

- **Экспортировать в файл**

  По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию программа экспортирует список устройств в файл формата CSV.

  **Свойства**По кнопке **Свойства** вы можете посмотреть и настроить параметры точки распространения, с которым взаимодействует устройство.

## См. также:

Настройка общих параметров Сервера администрирования .....685

## Общие параметры политик

### Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.

- **Политика для автономных пользователей**

  Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.

- **Неактивная политика**

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  - **Наследовать параметры из политики верхнего уровня**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

**Настройка событий**

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие.**

  Закладка **Критическое событие** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

На каждой закладке отображается список типов событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений (на странице 316), указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, на закладке **Предупреждение** вы можете настроить тип события **Произошел инцидент**. Такие события могут произойти, например, когда свободное место на диске точки распространения (см. стр. 88) меньше 2 ГБ (для установки программ и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошел инцидент**, выберите его и нажмите на кнопку **Свойства**. После этого вы можете указать, где хранить возникшие события и как о них уведомлять.

Если Агент администрирования обнаружил инцидент, вы можете управлять этим инцидентом с помощью параметров управляемого устройства (см. стр. 742).

Для выбора нескольких типов событий используйте клавиши **Shift** или **Ctrl**, для выбора всех типов используйте кнопку **Выбрать все**.

## См. также:

Контроль возникновения вирусных эпидемий .....687

## Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования:*

1. В дереве консоли выберите папку **Политики**.
2. В рабочей области папки выберите политику Агента администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.

Откроется окно свойств политики Агента администрирования.

### Общие

В разделе **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная политика**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Политика для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
  - **Неактивная политика**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры из политики верхнего уровня**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать**

**параметры родительской политики**.

Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

По умолчанию параметр выключен.

**Настройка событий**

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие.**

  Закладка **Критическое событие** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования.**
- **Предупреждение.**
- **Информационное сообщение.**

На каждой закладке отображается список типов событий и время хранения событий на Сервере администрирования по умолчанию (в днях). По кнопке **Свойства** можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений (на странице 316), указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, на закладке **Предупреждение** вы можете настроить тип события **Произошел инцидент**. Такие события могут произойти, например, когда свободное место на диске точки распространения (см. стр. 88) меньше 2 ГБ (для установки программ и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошел инцидент**, выберите его и нажмите на кнопку **Свойства**. После этого вы можете указать, где хранить возникшие события и как о них уведомлять.

Если Агент администрирования обнаружил инцидент, вы можете управлять этим инцидентом с помощью параметров управляемого устройства (см. стр. 742).

Для выбора нескольких типов событий используйте клавиши **Shift** или **Ctrl**, для выбора всех типов используйте кнопку **Выбрать все**.

**Параметры**

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

  Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования (см. стр. 453).

Обратите внимание, что программы безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждой программы безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Kaspersky Security Center установлен в качестве источника обновлений в задачах обновления.

По умолчанию параметр выключен.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Программа может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в программу безопасности (например, Kaspersky Endpoint Security для Windows). Передаваемая информация отображается в интерфейсе программы безопасности.

  Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политики.

  Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

  Если этот параметр включен, после того как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без необходимых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

  Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

  По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

  Если параметр включен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

  По умолчанию параметр выключен.

**Хранилища**

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения. Параметры раздела **Хранилища** доступны только для устройств под управлением Windows:

- **Информация об обновлениях Центра обновления Windows**

  Если параметр установлен, на Сервер администрирования отправляется информация об обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

  Иногда, даже если параметр выключен, обновления отображаются в свойствах

устройства в разделе **Применимые обновления**. Это может произойти, если, например, устройства организации имеют уязвимости, которые могут быть закрыты с помощью этих обновлений.

По умолчанию параметр включен. Доступен только для Windows.

- **Информация об уязвимостях в программах и соответствующих обновлениях**

  Если этот параметр включен, информация об уязвимостях в программах сторонних производителей (включая программное обеспечение Microsoft), обнаруженных на управляемых устройствах, и об обновлениях программного обеспечения для устранения уязвимостей (не включая программное обеспечение Microsoft) отправляется на Сервер администрирования.

  Выбор этого параметра (**Информация об уязвимостях программного обеспечения**) увеличивает нагрузку на сеть, загрузку диска Сервера администрирования и потребление ресурсов Агентом администрирования.

  По умолчанию параметр включен. Доступен только для Windows.

  Для управления обновлениями программного обеспечения Microsoft используйте параметр **Информация об обновлениях Центра обновления Windows**.

- **Информация о реестре оборудования**

Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить сведения об оборудовании. Сведения об оборудовании, полученные от виртуальных машин, могут быть неполными в зависимости от используемого гипервизора.

- **Информация об установленных программах**

  Если этот параметр включен, на Сервер администрирования отправляется информация о программах, установленных на клиентских устройствах.

  По умолчанию параметр включен.

- **Включить информацию о патче**

  Информация о патчах программ, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

  По умолчанию параметр включен. Доступен только для Windows.

**Обновления и уязвимости в программах**

В разделе **Обновления и уязвимости в программах** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей: Параметры раздела **Обновления и уязвимости в программах** доступны только для устройств под управлением Windows:

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Если этот параметр включен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

Если этот параметр выключен, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

По умолчанию параметр выключен.

- С помощью параметра **Разрешить пользователям управлять установкой обновлений Центра обновления Windows** вы можете ограничить обновления Windows, которые пользователи могут устанавливать на своих устройствах вручную, с помощью Центра обновления Windows.

  Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

  Выберите параметр из раскрывающегося списка:

  - **Устанавливать все применимые обновления Центра обновления Windows**

    Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

    Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

  - **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

  - **Запретить устанавливать обновления Центра обновления Windows**

    Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

    Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- В блоке параметров **Режим поиска обновлений Windows Update** можно выбрать режим поиска обновлений:
  - **Активный**

    Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от Агента Центра обновления Windows.

    Этот параметр вступает в силу только в том случае, если параметр **Соединяться с сервером обновлений для актуализации данных** задачи *Поиск уязвимостей и требуемых обновлений* включен.

    По умолчанию выбран этот вариант.

  - **Пассивный**

    Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

    Выберите этот параметр, если вы хотите получать обновления из кеша источника обновлений.

  - **Выключен**

    Если выбран этот вариант, Сервер администрирования не запрашивает информацию об обновлениях.

    Выберите этот параметр, если, например, вы хотите сначала протестировать обновления на локальном устройстве.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

  Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

  По умолчанию параметр включен.

**Управление перезагрузкой**

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления программы требуется перезагрузка операционной системы управляемого устройства. Параметры раздела **Управление перезагрузкой** доступны только для устройств под управлением Windows:

- **Не перезагружать операционную систему**

  Перезагрузка операционной системы не выполняется.

- **При необходимости перезагрузить операционную систему автоматически**

  При необходимости перезагрузка операционной системы выполняется автоматически.

- **Запрашивать у пользователя**

  Программа запрашивает у пользователя разрешение перезагрузить операционную систему.

  По умолчанию выбран этот вариант.

- **Периодичность напоминания о необходимости установки (мин)**

  Если этот параметр включен, программа запрашивает у пользователя разрешение на перезагрузку операционной системы с периодичностью, указанной в поле рядом с флажком. По умолчанию периодичность повторных запросов составляет 5 минут.

  Если этот параметр выключен, программа не запрашивает разрешение на перезагрузку повторно.

  По умолчанию параметр включен.

- **Принудительно перезагружать через (мин)**

  Если этот параметр включен, после запроса у пользователя операционная система перезагружается принудительно по истечении времени, указанного в поле рядом с флажком.

  Если этот параметр выключен, принудительная перезагрузка не выполняется.

По умолчанию параметр включен.

- **Принудительно закрывать программы в заблокированных сессиях через (мин)**

  Принудительное завершение работы программ, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа программ на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа программ на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

**Совместный доступ к рабочему столу Windows**

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу: Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

  Если параметр включен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

  - в журнале событий на удаленном устройстве;
  - в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
  - в базе событий Kaspersky Security Center.

  Аудит действий администратора доступен при выполнении следующих условий:

  - лицензия на Системное администрирование уже используется;
  - у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

Если параметр выключен, аудит действий администратора на удаленном устройстве выключен.

По умолчанию параметр выключен.

- **Маски файлов, чтение которых нужно отслеживать**

  В списке содержатся маски файлов. Когда аудит включен, программа отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

  В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен, программа отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

**Управление патчами и обновлениями**

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

  Если параметр выключен, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  По умолчанию параметр включен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

  Если флажок снят, офлайн-модель получения обновлений выключена. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых программ. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

  Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и

предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для программ на клиентских устройствах, но подключение не требуется для обновления.

Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

По умолчанию параметр включен.

**Подключения.**

Раздел **Подключения** включает три вложенных раздела:

- **Сеть.**
- **Профили соединений** (только для Windows и macOS).
- **Расписание соединений.**

В разделе **Сеть** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер. Доступны следующие параметры:

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Сжимать сетевой трафик**

    Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

    По умолчанию флажок установлен.

  - **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

    Если параметр включен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

    По умолчанию параметр включен.

  - **Использовать SSL**

    Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

    По умолчанию параметр включен.

  - **Использовать шлюз соединений точки распространения (при наличии) в параметрах подключения по умолчанию**

    Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

    По умолчанию параметр включен.

- **Использовать UDP-порт**

  Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

  Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный сетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

В разделе **Профили соединений** можно задать параметры сетевого местоположения, настроить профили подключения к Серверу администрирования, включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows и macOS:

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если параметр включен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. стр. 310). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

  Если параметр выключен, программы будут использовать активные политики.

  По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

**Точки распространения**

Раздел **Точки распространения** включает четыре подраздела:

- **Опрос сети.**
- **Параметры подключения к интернету.**
- **Прокси-сервер KSN.**
- **Обновления.**

В подразделе **Опрос сети** вы можете настроить автоматический опрос сети. Вы можете включить три типа опроса, то есть опрос сети, опрос IP-диапазонов и опрос Active Directory:

- **Разрешить опрос сети**

  Если параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

  Период обнаружения устройств для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период опроса Windows-доменов (мин)** и **Период опроса сети (мин)**.

  По умолчанию параметр выключен.

- **Разрешить опрос IP-диапазонов**

  Если параметр включен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если этот параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

  По умолчанию параметр выключен.

- **Использовать опрос Zeroconf (только на платформах Linux; заданные вручную диапазоны IP-адресов будут игнорироваться)**

- **Разрешить опрос Active Directory**

  Если параметр включен, Сервер администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если параметр выключен, точка не выполняет опрос Active Directory.

  Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

В разделе **Параметры подключения к интернету** можно настроить параметры доступа в интернет:

- **Использовать прокси-сервер**

  Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

  По умолчанию флажок снят.

- **Адрес прокси-сервера**

  Адрес прокси-сервера.

- **Номер порта**

  Номер порта, по которому будет выполняться подключение.

- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**

  Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.

- **Пароль**

  Пароль учетной записи, от имени которой будет запускаться задача.

В разделе **Прокси-сервер KSN** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security

Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены (см. стр. 830) в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Переслать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной-службе KSN/Локальному KSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или Локальному KSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или Локальный KSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к Локальному KSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к Локальному KSN.

- **TCP-порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

  Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

В подразделе **Обновления** вы можете указать, должен ли Агент администрирования загружать файлы различий (см. стр. 459), включив или выключив параметр **Загрузить файлы различий**. По умолчанию параметр включен.

### История ревизий

На закладке **История ревизий** можно посмотреть историю ревизий Агента администрирования (на стр. 811). Вы можете сравнивать ревизии, просматривать ревизии и выполнять другие операции, такие как сохранять ревизии в файл, откатывать ревизии, добавлять и изменять описания ревизий.

### Сравнение возможностей Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования для конкретной операционной системы.

*Таблица 68. Параметры политики Агента администрирования: сравнение по операционным системам*

| Раздел Политики | Windows | Mac | Linux |
|---|---|---|---|
| **Общие** | ✓ | ✓ | ✓ |
| **Настройка событий** | ✓ | ✓ | ✓ |
| **Параметры** | ✓ | ✓ | ✓<br>Доступны только параметры **Максимальный размер очереди событий (МБ)** и **Программа может получать расширенные данные политики на устройстве**. |
| **Хранилища** | ✓ | — | ✓<br>Доступны только параметры **Информация об установленных программах** и **Информация о реестре оборудования**. |
| **Обновления и уязвимости в программах** | ✓ | — | — |
| **Управление перезагрузкой** | ✓ | — | — |
| **Совместный доступ к рабочему столу Windows** | ✓ | — | — |
| **Управление патчами и обновлениями** | ✓ | — | — |
| **Подключения → Сеть** | ✓ | ✓ | ✓<br>Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** |
| **Подключения → Профили подключения** | ✓ | ✓ | — |

| Раздел Политики | Windows | Mac | Linux |
|---|---|---|---|
| **Подключения → Расписание соединений** | ✓ | ✓ | ✓ |
| **Точки распространения → Опрос сети** | ✓ | — | ✓<br>Доступен только раздел **Опрос IP-диапазонов**. |
| **Точки распространения] → Параметры подключения к интернету** | ✓ | ✓ | ✓ |
| **Точки распространения → KSN прокси-сервер** | ✓ | — | — |
| **Точки распространения → Обновления** | ✓ | — | — |
| **История ревизий** | ✓ | ✓ | ✓ |

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Об обновлениях программ сторонних производителей.....1284

# Управление учетными записями пользователей

Этот раздел содержит информацию об учетных записях и ролях пользователей, которые поддерживает программа. В разделе приведены инструкции по созданию учетных записей и ролей пользователей Kaspersky Security Center.

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. стр. 689). Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются (на стр. 766) и используются только внутри Kaspersky Security Center.

kaspersky

## В этом разделе



## Работа с учетными записями пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами учетных записей. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих пользователей при опросе сети организации.
- Учетные записи внутренних пользователей (см. стр. 689). Применяются для работы с виртуальными Серверами администрирования. Учетные записи внутренних пользователей создаются (на стр. 766) и используются только внутри Kaspersky Security Center.

Все учетные записи пользователей можно просмотреть в папке **Учетные записи пользователей** в дереве консоли. По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

Вы можете выполнять с учетными записями пользователей и группами учетных записей следующие действия:

- настраивать права доступа пользователей к функциям программы с помощью ролей (на стр. 771);
- рассылать сообщения пользователям с помощью электронной почты и SMS (на стр. 801);
- просматривать список мобильных устройств пользователя (на стр. 801);
- выписывать и устанавливать сертификаты на мобильные устройства пользователя (на стр. 802);
- просматривать список сертификатов, выписанных пользователю (на стр. 802);
- выключать двухэтапную проверку (на стр. 705) для учетной записи пользователя.

## Добавление учетной записи внутреннего пользователя

► *Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:*

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
2. В рабочей области нажмите на кнопку **Добавить пользователя**.
3. В открывшемся окне **Новый пользователь** укажите параметры нового пользователя:

   - Имя пользователя (  ).

     Пожалуйста, будьте внимательны при вводе имени пользователя. Вы не сможете его изменить после сохранения изменений.

   - **Описание.**
   - **Полное имя.**
   - **Основная электронная почта.**
   - **Основной номер телефона.**
   - **Пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:

     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A-Z);
       - нижний регистр (A-Z) (a-z);
       - числа (0-9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

     Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля" (на стр. 768).
     Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок  заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись, если вы хотите создать учетную запись заранее, но активировать ее позже.
- Установите флажок **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов (см. стр. 771) в области **Общий функционал**: **Права пользователей**.

4. Нажмите на кнопку **ОК**.

Созданная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

## Изменение учетной записи внутреннего пользователя

► *Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:*

1. В дереве консоли откройте папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. В рабочей области дважды щелкните учетную запись внутреннего пользователя, которую требуется изменить.
3. В открывшемся окне **Свойства: <имя пользователя>** измените параметры учетной записи пользователя:
   - **Описание.**
   - **Полное имя.**
   - **Основная электронная почта.**
   - **Основной номер телефона.**
   - **Пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:

     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A-Z);
       - нижний регистр (A-Z) (a-z);
       - числа (0-9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля" (на стр. 768).
Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. В списке учетных записей пользователей значок (  ) заблокированной учетной записи затемнен (недоступен). Вы можете разблокировать учетную запись, только сменив пароль.

- При необходимости установите флажок **Отключить учетную запись**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
- Установите флажок **Запрашивать пароль при изменении параметров учетной записи**, если вы хотите включить дополнительную защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, то для изменения параметров учетной записи пользователя требуется авторизация пользователя с правом Изменение списков управления доступом объектов (см. стр. 771) в области **Общий функционал**: **Права пользователей**.

4. Нажмите на кнопку **ОК**.

Измененная учетная запись пользователя отобразится в рабочей области папки **Учетные записи пользователей**.

## Изменение количества попыток ввода пароля

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля, следуя инструкции ниже.

► *Чтобы изменить количество попыток ввода пароля:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.
2. Перейдите к следующему разделу:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Если параметр SrvSplPpcLogonAttempts отсутствует в разделе реестра, создайте его. Тип значения параметра – DWORD.

   Этот параметр не создается по умолчанию при установке Kaspersky Security Center.
4. Укажите требуемое количество попыток в качестве значения параметра SrvSplPpcLogonAttempts.

5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
6. Перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

## Настройка проверки уникальности имени внутреннего пользователя

Вы можете настроить проверку уникальности имени внутреннего пользователя Kaspersky Security Center при его добавлении в программу. Проверка на уникальность имени внутреннего пользователя может выполняться только на виртуальном Сервере или главном Сервере, для которого создается учетная запись пользователя, или на всех виртуальных Серверах и главном Сервере. По умолчанию проверка на уникальность имени внутреннего пользователя выполняется на всех виртуальных Серверах и на главном Сервере администрирования.

► *Чтобы включить проверку уникальности имени внутреннего пользователя в рамках виртуального Сервера или главного Сервера:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000001.

   По умолчанию для этого ключа указано значение 0.
4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена только на том виртуальном Сервере, на котором был создан внутренний пользователь, или на главном Сервере, если пользователь был создан на главном Сервере.

► *Чтобы включить проверку уникальности имени внутреннего пользователя на всех виртуальных Серверах и главном Сервере:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск** → **Выполнить**.
2. Перейдите в раздел:
   - для 64-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\KLLIM
   - для 32-разрядной системы:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Для ключа LP_InterUserUniqVsScope (DWORD) установите значение 00000000.

   По умолчанию для этого ключа указано значение 0.

4. Перезапустите службу Сервера администрирования.

В результате проверка уникальности имени будет выполнена на всех виртуальных Серверах и на главном Сервере администрирования.

## Добавление группы безопасности

Вы можете добавлять группы безопасности (группы пользователей), гибко настраивать состав групп и доступ группы безопасности к разным функциям программы. Группам безопасности можно давать названия, соответствующие их назначению. Например, название может соответствовать расположению пользователей в офисе или названию структурного подразделения компании, к которому относятся пользователи.

Один пользователь может входить в состав нескольких групп безопасности. Учетная запись пользователя под управлением виртуального Сервера администрирования может входить только в группы безопасности этого виртуального Сервера и иметь права доступа только в рамках этого виртуального Сервера.

► *Чтобы добавить группу безопасности:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. Нажмите на кнопку **Добавить группу безопасности**.

   Откроется окно **Добавить группу безопасности**.

3. В окне **Добавить группу безопасности** в разделе **Общие** укажите имя группы.

   Имя группы не может превышать 255 символов и не может содержать символы *, <, >, ?, \, :, |. Имя группы должно быть уникальным.

   Вы можете ввести описание группы в поле ввода **Описание**. Заполнение поля **Описание** не является обязательным.

4. Нажмите на кнопку **ОК**.

Добавленная группа безопасности отобразится в папке **Учетные записи пользователей** в дереве консоли. Вы можете добавить пользователей (на стр. 770) в созданную группу.

## Добавление пользователя в группу

► *Чтобы добавить пользователя в группу:*

1. В дереве консоли выберите папку **Учетные записи пользователей**.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.

2. В списке учетных записей пользователей и групп выберите группу, в которую нужно добавить пользователя.

3. В окне свойств группы выберите раздел **Пользователи группы**, затем нажмите на кнопку **Добавить**.

   В результате откроется окно со списком пользователей.

4. В списке выберите пользователя или пользователей, которых нужно включить в состав группы.

5. Нажмите на кнопку **ОК**.

Пользователь добавлен в группу и отображается в списке пользователей группы.

kaspersky

## Настройка прав. Роли пользователей

Вы можете гибко настраивать доступ администраторов, пользователей и групп пользователей к разным функциям программы. Предоставлять пользователям права доступа к функциям программы можно двумя способами:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

*Роль пользователя* – это заранее созданный и настроенный набор прав доступа к функциям программы. Роль можно предоставить пользователю или группе пользователей. Применение ролей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к программе. Права доступа в роли настраивают в соответствии с "типовыми" задачами и служебными обязанностями пользователей. Например, роль пользователя может иметь права только на чтение и отправление информационных команд на мобильные устройства других пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В программе можно создавать неограниченное количество ролей.

Вы можете настроить доступ к различным функциям программы для следующих объектов:

- Серверов администрирования;
- групп администрирования;
- виртуальных Серверов администрирования.

### В этом разделе



### Права доступа к функциям программы

В таблице ниже приведены функции Kaspersky Security Center с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общий функционал**: функциональная область **Базовая функциональность**.

*Таблица 69. Права доступа к функциям программы*

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Управление группами администрирования.** | **Запись.** | • Добавление устройства в группу администрирования: **Запись.**<br>• Удаление устройства из состава группы администрирования: **Запись.**<br>• Добавление группы администрирования в другую группу администрирования: **Запись.**<br>• Удаление группы администрирования из другой группы администрирования: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Доступ к объектам независимо от их списков ACL.** | **Чтение.** | Получение доступа на чтение ко всем объектам: **Чтение.** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Базовая функциональность.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**.<br>• Получение мобильного протокола пользовательского сертификата (LWNGT): **Чтение.**<br>• Установка мобильного протокола пользовательского сертификата (LWNGT): **Запись.**<br>• Получить список | • Загрузка обновлений в хранилище Сервера администрирования.<br>• Рассылка отчетов.<br>• Распространение инсталляционных пакетов.<br>• Установка программ на подчиненные Серверы администрирования. | • Отчет о состоянии защиты.<br>• Отчет об угрозах.<br>• Отчет о наиболее заражаемых устройствах.<br>• Отчет о статусе антивирусных баз.<br>• Отчет об ошибках.<br>• Отчет о сетевых атаках.<br>• Сводный отчет о программах для защиты почтовых систем.<br>• Сводный отчет о программах для защиты периметра.<br>• Сводный отчет о типах программ.<br>• Отчет о пользователях зараженных | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | сетей, определенных NLA: **Чтение.**<br>• Добавить, изменить или удалить список сетей, определенных NLA: **Запись.**<br>• Просмотр списка контроля доступа групп: **Чтение.**<br>• Просмотрите журнал событий Kaspersky Event Log: **Чтение.** | | устройств.<br>• Отчет об инцидентах.<br>• Отчет о событиях.<br>• Отчет о работе точек распространения.<br>• Отчет о подчиненных Серверах администрирования.<br>• Отчет о событиях Контроля устройств.<br>• Отчет об уязвимостях.<br>• Отчет о запрещенных программах.<br>• Отчет о работе Веб-Контроля.<br>• Отчет о статусе шифрования управляемых | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | | | устройств.<br>• Отчет о статусе шифрования запоминающих устройств.<br>• Отчет об ошибках шифрования.<br>• Отчет о блокировании доступа к зашифрованным файлам.<br>• Отчет о правах доступа к зашифрованным устройствам.<br>• Отчет об эффективных правах пользователя.<br>• Отчет о правах. | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Удаленные объекты.** | • **Чтение.**<br>• **Запись.** | • Просмотр удаленных объектов в корзине: **Чтение.**<br>• Удаление объектов из корзины: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Обработка событий.** | • **Удаление событий.**<br>• **Изменение параметров уведомления о событиях.**<br>• **Изменение параметров записи событий в журнал событий.**<br>• **Запись.** | • Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий.**<br>• Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях.**<br>• Удаление событий: **Удаление событий.** | Отсутствует. | Отсутствует. | Параметры:<br>• Параметры вирусной атаки: количество обнаружений вирусов, необходимое для создания события вирусной атаки.<br>• Параметры вирусной атаки: период для оценки обнаружения вирусов.<br>• Максимальное количество событий, хранящихся в базе данных.<br>• Период хранения событий удаленных устройств. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Операции с Сервером администрирования.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Изменение списков ACL объекта.**<br>• **Выполнение действий над выборками устройств.** | • Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись.**<br>• Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись.**<br>• Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись.**<br>• Изменение портов Веб-сервера для распростр | • Резервное копирование данных Сервера администрирования.<br>• Обслуживание базы данных. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | анения автономных пакетов: **Запись.**<br>• Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись.**<br>• Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись.**<br>• Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись.**<br>• Укажите максимал | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | ьное количество событий, хранящихся в базе данных Сервера администрирования. **Запись.**<br>• Укажите максимальное количество событий, которое может отправлять Сервер администрирования. **Запись.**<br>• Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись.** | | | |
| **Общие функции**: **Развертывание программ "Лаборатории Касперского".** | • **Управление патчами "Лаборатории Касперского".**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.** | Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского".** | Отсутствует. | • Отчет об использовании лицензионных ключей виртуальным Сервером администрат | Инсталляционный пакет: "Лаборатория Касперского". |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | • **Выполнение действий над выборками устройств.** | | | рирования.<br>• Отчет о версиях программ "Лаборатории Касперского".<br>• Отчет о несовместимых программах.<br>• Отчет о версиях обновлений модулей программ "Лаборатории Касперского".<br>• Отчет о развертывании защиты. | |
| **Общие функции**: **Управление лицензионными ключами.** | • **Экспорт файл ключа.**<br>• **Запись.** | • Экспорт файл ключа: **Экспорт файл ключа.**<br>• Изменение параметров лицензионного ключа Сервера администр | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | ирования: **Запись.** | | | |
| **Общие функции**: **Управление отчетами.** | • **Чтение.**<br>• **Запись.** | • Создание отчетов для объектов независимо от их списков ACL: **Запись.**<br>• Выполнять отчеты независимо от их списков ACLs: **Чтение.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Иерархия Серверов администрирования** | **Настройка иерархии Серверов администрирования** | Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Права пользователя.** | **Изменение списков ACL объекта.** | • Изменение свойств Безопасности любого объекта: **Изменение списков ACL объекта.**<br>• Управление ролями пользователей: **Изменение списков ACL объекта.**<br>• Управление внутренними пользователями: **Изменение списков ACL объекта.**<br>• Управление группами безопасности: **Изменение списков ACL объекта.**<br>• Управление псевдонимами: **Изменение списков ACL объекта.** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **виртуальные Серверы администрирования;** | • **Управление виртуальными Серверами администрирования.**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Получение списка виртуальных Серверов администрирования: **Чтение.**<br>• Получение информации о виртуальном Сервере администрирования: **Чтение.**<br>• Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования.**<br>• Перемещение виртуального Сервера администрирования в другую группу: | Отсутствует. | Отчет о результатах установки обновлений стороннего ПО. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **Управление виртуальными Серверами администрирования.**<br>• Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования.** | | | |
| **Общие функции**: **Управление ключами шифрования** | • **Чтение.**<br>• **Запись.** | • Экспорт ключей шифрования: **Чтение.**<br>• Импорт ключей шифрования: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Управление мобильными устройствами**: **Общие** | • **Подключение новых устройств.**<br>• **Отправка только информационных команд на мобильные устройства.**<br>• **Отправка команд на мобильные устройства.**<br>• **Управление сертификатами.**<br>• **Чтение.**<br>• **Запись.** | • Получение восстановленных данных службы управления ключами: **Чтение.**<br>• Удаление сертификатов пользователей: **Управление сертификатами.**<br>• Получение публичной части сертификата пользователя: **Чтение.**<br>• Проверка, включена ли инфраструктура открытых ключей: **Чтение.**<br>• Проверка учетной записи инфраструктуры открытых ключей: **Чтение.** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | • Получение шаблонов инфраструктуры открытых ключей: **Чтение.**<br>• Получение шаблонов инфраструктуры открытых ключей с помощью расширенного использования ключа (EKU) сертификата: **Чтение.**<br>• Проверка, не отозван ли сертификат инфраструктуры открытых ключей: **Чтение.**<br>• Обновление параметров выпуска сертификатов пользователя: **Управление** | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **сертификатами.**<br>• Получение параметров выпуска сертификатов пользователя: **Чтение.**<br>• Получение пакетов по названию и версиям программ: **Чтение.**<br>• Установка или отмена сертификатов пользователя: **Управление сертификатами.**<br>• Обновление сертификата пользователя: **Управление сертификатами.**<br>• Установка тега для сертификата пользователя: | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **Управление сертификатами.**<br>• Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: **Подключение новых устройств.** | | | |
| **Управление системой**: **Подключения.** | • **Запуск RDP-сессий.**<br>• **Подключение к существующим RDP-сессиям.**<br>• **Туннелирование.**<br>• **Сохранение файлов с устройства на рабочем** | • Создание сеанса совместного доступа к рабочему столу: **Право на создание сеанса совместного доступа к рабочему столу.**<br>• Создание RDP-сессии: | Отсутствует. | Отчет о пользователях устройства. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | **месте администратора.**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | **Подключение к существующим RDP-сессиям.**<br>• Создание туннеля: **Туннелирование.**<br>• Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте администратора.** | | | |
| **Управление системой**: **Инвентаризация оборудования** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Получение или экспорт объектов инвентаризации оборудования: **Чтение.**<br>• Добавление, установка или удаление объектов инвентаризации оборудования: **Запись.** | Отсутствует. | • Отчет о реестре оборудования.<br>• Отчет об изменении конфигурации.<br>• Отчет об оборудовании. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Управление системой**: **Управление доступом в сеть.** | • **Чтение.**<br>• **Запись.** | • Просмотр параметров Cisco: **Чтение.**<br>• Изменение параметров Cisco: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Управление системой**: **Развертывание операционной системы.** | • **Развертывание PXE-серверов.**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Развертывание PXE-серверов: **Развертывание PXE-серверов.**<br>• Просмотр списка PXE-серверов: **Чтение.**<br>• Запуск или остановка процесс установки на PXE-клиентах: **Выполнение.**<br>• Управление драйверами для среды WinPE и образов операционной системы: **Запись.** | Создание инсталляционного пакета на основе образа ОС эталонного устройства. | Отсутствует. | Инсталляционный пакет: Образ операционной системы. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Управление системой**: **Системное администрирование.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Просмотр свойства патчей сторонних производителей: **Чтение.**<br>• Изменение свойства патчей сторонних производителей: **Запись.** | • Выполнение синхронизации обновлений Центра обновления Windows.<br>• Установка обновлений Центра обновления Windows.<br>• Закрытие уязвимостей.<br>• Установка требуемых обновлений и закрытия уязвимостей. | Отчет об обновлениях ПО. | Отсутствует. |
| **Управление системой**: **Удаленная установка** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение.**<br>• Изменение Системного | Отсутствует. | Отсутствует. | Инсталляционные пакеты:<br>• "Пользовательская программа".<br>• Инсталляционный пакет. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | администрирования на основе свойств инсталляционного пакета: **Запись.** | | | |
| **Управление системой**: **Инвентаризация программ.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | Отсутствует. | Отсутствует. | • Отчет об установленных программах.<br>• Отчет об истории реестра программ.<br>• Отчет о состоянии групп лицензионных программ.<br>• Отчет о лицензионных ключах сторонних программ. | Отсутствует. |

kaspersky

## Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям программы (на стр. 771).

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center начиная с версии 11). Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

*Таблица 70. Примеры ролей для определенных должностей*

| Роль | Комментарий |
|---|---|
| Аудитор | Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права **Чтение** и **Запись** для области **Удаленные объекты**). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации. |
| Контролер | Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации. |
| Специалист по безопасности | Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации. |

В таблице ниже приведены права для каждой предопределенной роли пользователя.

*Таблица 71. Права предопределенных ролей пользователей*

| Роль | Описание |
|---|---|
| Администратор Сервера администрирования | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Обработка событий.**<br>  • **Иерархия Серверов администрирования**<br>  • **виртуальные Серверы администрирования;** |

| Роль | Описание |
| --- | --- |
| | • **Управление системой**:<br>  • **Подключения.**<br>  • **Инвентаризация оборудования**<br>  • **Инвентаризация программ.**<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Оператор Сервера администрирования | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **виртуальные Серверы администрирования;**<br>• **Управление системой**:<br>  • **Подключения.**<br>  • **Инвентаризация оборудования**<br>  • **Инвентаризация программ.** |
| Аудитор | Разрешает все операции в функциональной области **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Удаленные объекты.**<br>• **Управление отчетами.**<br>Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации. |
| Администратор установки программ | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Развертывание программ "Лаборатории Касперского".**<br>  • **Управление лицензионными ключами.**<br>• **Управление системой**:<br>  • **Развертывание операционной системы.**<br>  • **Системное администрирование.**<br>  • **Удаленная установка**<br>  • **Инвентаризация программ.**<br>Предоставляет права на **Чтение** и **Выполнение** в области **Общий функционал**: функциональная область **Виртуальные Серверы администрирования**. |

| Роль | Описание |
|---|---|
| Оператор установки программ | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Развертывание программ "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области).<br>  • **виртуальные Серверы администрирования;**<br>• **Управление системой**:<br>  • **Развертывание операционной системы.**<br>  • **Системное администрирование.**<br>  • **Удаленная установка**<br>  • **Инвентаризация программ.** |
| Администратор Kaspersky Endpoint Security | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• Область Kaspersky Endpoint Security, включая все функции.<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Оператор Kaspersky Endpoint Security | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• Область Kaspersky Endpoint Security, включая все функции. |
| Главный администратор | Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Управление отчетами.**<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Главный оператор | Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Удаленные объекты.**<br>  • **Операции с Сервером администрирования.**<br>  • **Развертывание программ "Лаборатории Касперского"**<br>  • **Виртуальные Серверы администрирования**<br>• **Управление мобильными устройствами: Общие**<br>• **Управление системой**, включая все функции.<br>• Область Kaspersky Endpoint Security, включая все функции. |

| Роль | Описание |
|---|---|
| Администратор управления мобильными устройствами | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• **Управление мобильными устройствами: Общие** |
| Оператор управления мобильными устройствами | Предоставляет права на **Чтение** и **Выполнение** в области **Общий функционал**: функциональная область **Базовая функциональность**.<br>Предоставляет права на **Чтение** и **Отправление только информационных команд на мобильные устройства** в следующих функциональных областях: **Управление мобильными устройствами**: функциональная область **Общие**. |
| Специалист по безопасности | Разрешает все операции в следующих функциональных областях: **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Управление отчетами.**<br>Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой:** функциональная область **Подключения**.<br>Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации. |
| Пользователь Self Service Portal | Разрешает все операции в области **Управление мобильными устройствами**: Функциональная область **Self Service Portal**. Эта функция не поддерживается в версиях программы Kaspersky Security Center 11 и выше. |
| Контролер | Предоставляет права на **Чтение** в области **Общий функционал**: **Доступ к объектам независимо от их списков ACL** и **Общий функционал**: функциональная область **Управление отчетами**.<br>Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации. |
| Администратор Системного администрирования | Разрешает все операции в области **Общий функционал**: функциональные области **Базовая функциональность** и **Управление системой** (включая все функции). |
| Оператор Системного администрирования | Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общий функционал**: функциональные области **Базовая функциональность** и **Управление системой** (включая все функции). |

## Добавление роли пользователя

► *Чтобы добавить роль пользователя:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

3. В окне свойства Сервера администрирования перейдите в раздел **Роли пользователей** и нажмите на кнопку **Добавить**.

   Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности** (на стр. 685).

4. В окне **Новая роль** настройте параметры роли:

   - Выберите раздел **Общие** и укажите имя роли.

     Имя роли не может превышать 100 символов.

   - В разделе **Права** настройте набор прав, установив флажки **Разрешить** и **Запретить** напротив функций программы.

   Если вы работаете на главном Сервере администрирования, вы можете включить параметр **Передать список ролей подчиненному Серверу администрирования** (на стр. 799).

5. Нажмите на кнопку **ОК**.

Роль добавлена.

Роли пользователей, созданные для Сервера администрирования, отображаются в окне свойств Сервера в разделе **Роли пользователей**. Вы можете изменять и удалять роли пользователей, а также назначать роли группам пользователей (на стр. 797) или отдельным пользователям.

## Назначение роли пользователю или группе пользователей

► *Чтобы назначить роль пользователю или группе пользователей:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. стр. 685).

4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которой нужно присвоить роль.

   Если пользователь или группа отсутствует в поле, добавьте их по кнопке **Добавить**.

   При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.

5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.

6. В окне **Роли пользователей** выберите роль для группы пользователей.
7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

## Назначение прав пользователям или группам пользователей

Вы можете назначить права пользователям или группам пользователей, чтобы использовать различные возможности Сервера администрирования и программ "Лаборатории Касперского", для которых у вас есть плагины управления, например, Kaspersky Endpoint Security для Windows.

► *Чтобы назначить права пользователю или группе пользователей:*

1. В дереве консоли выполните одно из следующих действий:
   - Раскройте узел **Сервер администрирования** и выберите подпапку с именем требуемого Сервера администрирования.
   - Выберите группу администрирования.
2. В контекстном меню Сервера администрирования или группы администрирования выберите пункт **Свойства**.
3. В открывшемся окне свойств Сервера администрирования (или окне свойств групп администрирования) выберите раздел **Безопасность**.

   Раздел **Безопасность** доступен, если в окне параметров интерфейса установлен флажок **Отображать разделы с параметрами безопасности** (см. стр. 685).
4. В разделе **Безопасность** в списке **Имена групп или пользователей** выберите пользователя или группу пользователей.
5. В списке прав в нижней части окна, на закладке **Права** настройте права для пользователей или групп:
   a. Нажмите на значок плюс (+), чтобы раскрыть узел в списке, и назначьте права.
   b. Установите флажки **Разрешить** и **Запретить** рядом с требуемыми правами.

      *Пример 1:* Раскройте узел **Доступ к объектам независимо от их списков ACL** или узел **Удаленные объекты**, и выберите **Чтение**.

      *Пример 2:* Раскройте узел **Базовая функциональность** и выберите **Изменение**.
6. После того как вы настроили набор прав, нажмите на кнопку **Применить**.

Набор прав для пользователя или группа пользователей настроен.

Права Сервера администрирования (или группы администрирования) разделены на следующие области:

- Общие функции:
  - Управление группами администрирования (только для Kaspersky Security Center 11 и выше).
  - Доступ к объектам независимо от их списков ACL (только для Kaspersky Security Center 11 и выше).
  - Базовая функциональность.
  - Удаленные объекты (только для Kaspersky Security Center 11 и выше).
  - Обработка событий.

    - Операции с Сервером администрирования (только в окне свойств Сервера администрирования).
    - Развертывание программ "Лаборатории Касперского".
    - Управление лицензионными ключами.
    - Управление отчетами (только для Kaspersky Security Center 11 и выше).
    - Иерархия Серверов.
    - Права пользователей.
    - Виртуальные Серверы администрирования.
- Управление мобильными устройствами:
    - Общие
- Управление системой:
    - Подключения.
    - Инвентаризация оборудования.
    - Управление доступом в сеть.
    - Развертывание операционной системы.
    - Управление уязвимостями и патчами.
    - Удаленная установка.
    - Инвентаризация программ.

Если для права не выбрано ни **Разрешить**, ни **Запретить**, оно считается *неопределенным*: право отклоняется до тех пор, пока оно не будет явно отклонено или разрешено для пользователя.

Права пользователей являются суммой:

- собственных прав пользователя;
- прав всех ролей, назначенных пользователю;
- прав всех групп безопасности, в которые входит пользователь;
- прав всех ролей, назначенных группам, в которые входит пользователь.

Если хотя бы в одном наборе прав есть запрещенное право (для права установлен флажок **Запретить**), тогда для пользователя это право запрещено, даже если в других наборах прав оно разрешено или не определено.

## Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить программы для автоматического распространения ролей пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

► *Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования:*

1. Откройте главное окно программы.
2. Выполните одно из следующих действий:

- В дереве консоли в контекстном меню требуемого Сервера администрирования выберите пункт **Свойства**.
- Если у вас есть активная политика Сервера администрирования, в рабочей области папки **Политики** в контекстном меню этой политики выберите пункт **Свойства**.

3. В окне свойств Сервера администрирования или в окне свойств политики перейдите в раздел **Роли пользователей**.

> Раздел **Роли пользователей** доступен, если включен параметр **Отображать разделы с параметрами безопасности** (на стр. 685).

4. Включите параметр **Передать список ролей подчиненному Серверу администрирования**.
5. Нажмите на кнопку **ОК**.

Программа копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью значка замок (). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~~1, ~~2 (номер может быть случайным).

Если отключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования становятся независимыми, их можно изменять или удалять.

## Назначение пользователя владельцем устройства

Вы можете назначить пользователя владельцем устройства, чтобы "закрепить" устройство за этим пользователем. При необходимости выполнить какие-либо действия с устройством (например, обновить аппаратное обеспечение) администратор может проинформировать владельца устройства и согласовать действия с ним.

► *Чтобы назначить пользователя владельцем устройства:*

1. В дереве консоли откройте папку **Управляемые устройства**.
2. В рабочей области папки на закладке **Устройства** выберите устройство, для которого нужно назначить владельца.
3. В контекстном меню узла Сервера администрирования выберите пункт **Свойства**.

4. В окне свойств устройства выберите раздел **Информация о системе** → **Сеансы**.
5. Нажмите на кнопку **Назначить** рядом с полем **Владелец устройства**.
6. В окне **Пользовательская выборка** выберите пользователя, которого нужно назначить владельцем устройства и нажмите на кнопку **ОК**.
7. Нажмите на кнопку **ОК**.

В результате владелец устройства будет назначен. По умолчанию поле **Владелец устройства** заполнено значением из Active Directory и обновляется при каждом опросе Active Directory (на стр. 329). Вы можете просмотреть список владельцев устройств в отчете **Отчет о владельцах устройств**. Отчет можно создать с помощью мастера создания отчетов (на стр. 584).

## Рассылка сообщений пользователям

► *Чтобы отправить сообщение пользователю по электронной почте:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
2. В контекстном меню пользователя выберите **Отправить сообщение по электронной почте**.
3. Заполните необходимые поля в окне **Сообщение для пользователя** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на электронную почту, указанную в свойствах пользователя.

► *Чтобы отправить SMS-сообщение пользователю:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.
2. В контекстном меню пользователя выберите **Отправить SMS-сообщение**.
3. Заполните необходимые поля в окне **Текст SMS** и нажмите на кнопку **ОК**.

В результате сообщение будет отправлено на мобильное устройство, номер которого указан в свойствах пользователя.

## Просмотр списка мобильных устройств пользователя

► *Чтобы просмотреть список мобильных устройств пользователя:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Мобильные устройства**.

В разделе **Мобильные устройства** можно просмотреть список мобильных устройств пользователя и информацию о мобильных устройствах. По кнопке **Экспортировать в файл** можно сохранить список мобильных устройств в файле.

## Установка сертификата пользователю

Вы можете установить пользователю сертификаты трех типов:

- общий сертификат, необходим для идентификации мобильного устройства пользователя;
- почтовый сертификат, необходим для настройки корпоративной почты на мобильном устройстве пользователя;
- VPN сертификат, необходим для настройки виртуальной частной сети на мобильном устройстве пользователя.

► *Чтобы выписать сертификат пользователю и установить его:*

1. В дереве консоли откройте папку **Учетные записи пользователей** и выберите учетную запись пользователя.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Установить сертификат**.

Будет запущен мастер установки сертификата. Следуйте далее указаниям мастера.

В результате работы мастера установки сертификата сертификат будет создан и установлен пользователю. Список установленных сертификатов пользователя можно просмотреть и экспортировать в файл (на стр. 802).

## Просмотр списка сертификатов, выписанных пользователю

► *Чтобы просмотреть список всех сертификатов, выписанных пользователю:*

1. В дереве консоли в папке **Учетные записи пользователей** выберите пользователя.

   По умолчанию папка **Учетные записи пользователей** вложена в папку **Дополнительно**.
2. В контекстном меню учетной записи пользователя выберите пункт **Свойства**.
3. В окне свойств учетной записи пользователя выберите раздел **Сертификаты**.

В разделе **Сертификаты** можно просмотреть список сертификатов пользователя и информацию о сертификатах. По кнопке **Экспортировать в файл** можно сохранить список сертификатов в файле.

## Об администраторе виртуального Сервера

При необходимости можно создать несколько учетных записей администраторов виртуального Сервера.

Администратор виртуального Сервера администрирования является внутренним пользователем Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

kaspersky

# Дистанционная установка операционных систем и программ

Kaspersky Security Center позволяет централизованно создавать образы операционных систем и разворачивать их на клиентских устройствах по сети, а также выполнять удаленную установку программ "Лаборатории Касперского" или других производителей программного обеспечения.

Для создания образов операционных систем необходимо установить Windows ADK https://go.microsoft.com/fwlink/?linkid=2165884 и средства дополнения Windows PE для Windows ADK на Сервере администрирования https://go.microsoft.com/fwlink/?linkid=2166133. Рекомендуется установить последние версии Windows ADK и дополнения Windows PE для Windows ADK. Вы можете создать образ любой версии операционной системы Windows, отвечающей требованиям Kaspersky Security Center (см. стр. 69).

### Захват образов операционных систем

Kaspersky Security Center может выполнять захват образов операционных систем устройств и доставлять эти образы на Сервер администрирования. Такие образы операционных систем хранятся на Сервере администрирования в специальной папке. Снятие и создание образа операционной системы эталонного устройства выполняется с помощью задачи создания инсталляционного пакета (на стр. 809).

Функциональность захвата образа операционной системы имеет следующие особенности:

- Образ операционной системы нельзя снимать с устройства, на котором установлен Сервер администрирования.
- Во время снятия образа операционной системы происходит обнуление параметров эталонного устройства утилитой sysprep.exe. В случае необходимости восстановления параметров эталонного устройства в мастере создания образа операционной системы необходимо установить флажок **Сохранять резервную копию состояния устройства**.
- В процессе снятия образа выполняется перезагрузка эталонного устройства.

### Развертывание образов операционных систем на новых устройствах

Вы можете использовать полученные образы для развертывания на новых устройствах в сети, на которых еще не была установлена операционная система. Для этой цели используется технология Preboot eXecution Environment (PXE). Вы назначаете устройство в сети, которое будет использоваться в качестве PXE-сервера. Это устройство должно отвечать следующим требованиям:

- на устройстве должен быть установлен Агент администрирования;
- на устройстве не должен работать DHCP-сервер, так как PXE-сервер использует те же порты, что и DHCP;
- в сегменте сети, в который входит устройство, не должно быть других PXE-серверов.

Для развертывания операционной системы должны быть выполнены следующие условия:

- на устройстве должна быть установлена сетевая карта;
- устройство должно быть подключено к сети;
- при загрузке устройства в BIOS необходимо выбрать параметр загрузки по сети.

Развертывание операционной системы выполняется в следующей последовательности:

1. PXE-сервер устанавливает соединение с новым клиентским устройством при загрузке клиентского устройства.
2. Клиентское устройство включается в среду Windows Preinstallation Environment (WinPE).

Для включения устройства в среду WinPE может потребоваться настройка состава драйверов для среды WinPE.

3. Клиентское устройство регистрируется на Сервере администрирования.
4. Администратор назначает клиентскому устройству инсталляционный пакет с образом операционной системы.

Администратор может добавлять необходимые драйверы в инсталляционный пакет с образом операционной системы. Администратор также может указывать конфигурационный файл с параметрами операционной системы (файл ответов), которые должны применяться во время установки.

5. Выполняется развертывание операционной системы на клиентском устройстве.

Администратор может вручную указать MAC-адреса еще не подключившихся клиентских устройств и назначить им инсталляционный пакет с образом операционной системы. Когда указанные клиентские устройства подключаются к PXE-серверу, автоматически выполняется установка операционной системы на этих устройствах.

**Развертывание образов операционных систем на устройствах с уже установленной операционной системой**

Развертывание образов операционной системы на клиентских устройствах, на которых уже установлена рабочая операционная система, выполняется с помощью задачи удаленной установки для наборов устройств.

**Установка программ "Лаборатории Касперского" и других производителей программного обеспечения**

Администратор может создавать инсталляционные пакеты любых программ, включая программы, указанные пользователем, и устанавливать эти программы на клиентские устройства с помощью задачи удаленной установки.

## В этом разделе

## Создание образов операционных систем

Создание образов операционных систем выполняется при помощи задачи снятия образа операционной системы эталонного устройства.

► *Чтобы создать задачу снятия образа операционной системы:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет с образом операционной системы**.
4. Следуйте далее указаниям мастера.

   В результате работы мастера создается задача Сервера администрирования **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. Задачу можно просмотреть в папке **Задачи**.

В результате выполнения задачи **Создание инсталляционного пакета на основе образа ОС эталонного устройства** создается инсталляционный пакет, который можно использовать для развертывания операционной системы на клиентских устройствах с помощью PXE-сервера или задачи удаленной установки. Просмотреть инсталляционный пакет можно в папке **Инсталляционные пакеты**.

## Установка образов операционных систем

Kaspersky Security Center позволяет разворачивать на устройства сети организации wim-образы настольных и серверных версий операционных систем Windows®.

Образ операционной системы, пригодный для развертывания средствами Kaspersky Security Center, может быть получен следующими способами:

- импортом из файла install.wim, который входит в состав дистрибутива Windows;
- захватом образа с эталонного устройства.

Поддерживаются два сценария развертывания образа операционной системы:

- развертывание на "чистое" устройство, то есть на устройство без установленной на нем операционной системы;
- развертывание на устройство, работающее под управлением операционной системы Windows.

В составе Сервера администрирования неявно присутствует служебный образ WinPE (Windows Preinstallation Environment), который всегда используется как при захвате, так и во время развертывания образов операционной системы. В WinPE следует добавить все драйверы, необходимые для правильной работы всех устройств. Как правило, требуется добавить драйверы чипсета, необходимые для работы сетевого интерфейса Ethernet.

Для реализации сценариев развертывания и захвата образов должны быть выполнены следующие требования:

- На Сервер администрирования должен быть установлен Windows Automated Installation Kit (WAIK) версии 2.0 и выше или Windows Assessment and Deployment Kit (WADK). Если предполагаются работы по установке или захвату образов на Windows XP, следует установить WAIK.
- В сети, в которой расположено устройство, должен присутствовать DHCP-сервер.

- Папка общего доступа Сервера администрирования должна быть доступна для чтения из сети, в которой находится устройство. Если папка общего доступа расположена на Сервере администрирования, то доступ нужен для учетной записи KlPxeUser (эта учетная запись создается автоматически на этапе работы инсталлятора Сервера администрирования). Если папка расположена вне Сервера администрирования, то доступ нужен для всех.

При выборе образа операционной системы для установки администратор должен явно указать архитектуру процессора устройства: x86 или x86-64.

## Настройка адреса прокси-сервера KSN

По умолчанию доменное имя Сервера администрирования совпадает с адресом прокси-сервера KSN. При изменении доменного имени для Сервера администрирования необходимо указать правильный адрес прокси-сервера KSN, чтобы предотвратить потерю связи между устройствами и KSN.

► *Чтобы настроить адреса прокси-сервера KSN:*

1. В дереве консоли перейдите в раздел **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета выберите пункт **Свойства**.
3. В открывшемся окне укажите новый адрес прокси-сервера KSN на закладке **Общие**.
4. Нажмите на кнопку **Применить**.

С этого момента указанный адрес используется как адрес прокси-сервера KSN.

### См. также

Kaspersky Security Network и Kaspersky Private Security Network .....829

## Добавление драйверов для среды предустановки Windows (WinPE)

► *Чтобы добавить драйверы для среды предустановки Windows (WinPE):*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. В рабочей области папки **Развертывание образов устройств** нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Настроить состав драйверов для среды предустановки Windows (WinPE)**.

   В результате откроется окно **Драйверы для среды предустановки Windows**.
3. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор драйвера**.
4. В окне **Выбор драйвера** выберите драйвер из списка.

   Если необходимый драйвер отсутствует в списке, нажмите на кнопку **Добавить** и в открывшемся окне **Добавление драйвера** укажите имя драйвера и папку дистрибутива драйвера.

   Вы можете выбрать папку по кнопке **Обзор**.

   В окне **Добавление драйвера** нажмите на кнопку **ОК**.
5. В окне **Выбор драйвера** нажмите на кнопку **ОК**.

Драйвер будет добавлен в хранилище Сервера администрирования. Добавленный в хранилище драйвер отображается в окне **Выбор драйвера**.

6. В окне **Драйверы для среды предустановки Windows** нажмите на кнопку **ОК**.

Драйвер будет добавлен в среду предустановки Windows (WinPE).

## Добавление драйверов в инсталляционный пакет с образом операционной системы

► *Чтобы добавить драйверы в инсталляционный пакет с образом операционной системы:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.
3. В окне свойств инсталляционного пакета выберите раздел **Дополнительные драйверы**.
4. В разделе **Дополнительные драйверы** нажмите на кнопку **Добавить**.

   Откроется окно **Выбор драйвера**.
5. В окне **Выбор драйвера** выберите драйверы, которые вы хотите добавить в инсталляционный пакет с образом операционной системы.

   Новые драйверы можно добавить в хранилище Сервера администрирования при нажатии на кнопку **Добавить** в окне **Выбор драйвера**.
6. Нажмите на кнопку **ОК**.

Добавленные драйверы отображаются в разделе **Дополнительные драйверы** в окне свойств инсталляционного пакета с образом операционной системы.

## Настройка параметров утилиты sysprep.exe

Утилита sysrep.exe используется для подготовки устройства к созданию с него образа операционной системы.

► *Чтобы настроить параметры утилиты sysprep.exe:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета с образом операционной системы выберите пункт **Свойства**.

   Откроется окно свойств инсталляционного пакета.
3. В окне свойств инсталляционного пакета выберите раздел **Параметры sysprep.exe**.
4. В разделе **Параметры sysprep.exe** укажите конфигурационный файл, который будет использоваться при развертывании операционной системы на клиентском устройстве:
   - **Использовать конфигурационный файл по умолчанию**. Выберите этот вариант, чтобы использовать файл ответов, создаваемый по умолчанию во время снятия образа операционной системы.

- **Задать пользовательские значения основных параметров**. Выберите этот вариант, чтобы задать значения параметров с помощью пользовательского интерфейса.
- **Задать конфигурационный файл**. Выберите этот вариант, чтобы использовать собственный файл ответов.

5. Нажмите на кнопку **Применить**, чтобы внесенные изменения вступили в силу.

## Развертывание операционных систем на новых устройствах в сети

► *Чтобы развернуть операционную систему на новых устройствах, на которых еще не установлена операционная система:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Развертывание образов устройств**.
2. Нажмите на кнопку **Дополнительные действия** и в раскрывающемся списке выберите пункт **Управлять списком PXE-серверов в сети**.

   Откроется окно **Свойства:** Откроется окно **Развертывание образов устройств** на разделе **PXE-серверы**.
3. В разделе **PXE-серверы** нажмите на кнопку **Добавить** и в открывшемся окне **PXE-серверы** выберите устройство, которое будет использоваться как PXE-сервер.

   Добавленное устройство отобразится в разделе PXE-серверы.
4. В разделе **PXE-серверы** выберите PXE-сервер и нажмите на кнопку **Свойства**.
5. В окне свойств выбранного PXE-сервера в разделе **Параметры подключения к PXE-серверу** выполните настройку параметров подключения Сервера администрирования к PXE-серверу.
6. Выполните загрузку клиентского устройства, на котором вы хотите развернуть операционную систему.
7. В среде BIOS клиентского устройства выберите вариант установки Network boot.

   Клиентское устройство подключается к PXE-серверу и отображается в рабочей области папки **Развертывание образов устройств**.
8. В блоке **Действия** по ссылке **Назначить инсталляционный пакет** выберите инсталляционный пакет, который будет использоваться для установки операционной системы на выбранное устройство.

   После добавления устройства и назначения для него инсталляционного пакета развертывание операционной системы на этом устройстве начинается автоматически.
9. Для отмены развертывания операционной системы на клиентском устройстве воспользуйтесь ссылкой **Отменить установку образов ОС** в блоке **Действия**.

► *Чтобы добавить устройства по MAC-адресу, выполните одно из следующих действий:*

- по ссылке **Добавить MAC-адрес устройства** в папке **Развертывание образов устройств** откройте окно **Новое устройство** и укажите MAC-адрес устройства, которое вы хотите добавить;
- по ссылке **Импортировать MAC-адреса устройств из файла** в папке **Развертывание образов устройств** выберите файл, содержащий список MAC-адресов всех устройств, на которых вы хотите развернуть операционную систему.

### См. также:

Основной сценарий установки.....92

## Развертывание операционных систем на клиентских устройствах

► *Чтобы выполнить развертывание операционной системы на клиентских устройствах с уже установленной операционной системой:*

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет с образом операционной системы.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки операционной системы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

## Создание инсталляционных пакетов программ

► *Чтобы создать инсталляционный пакет программы:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.
2. По кнопке **Создать инсталляционный пакет** запустите мастер создания инсталляционного пакета.
3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на одну из кнопок:
   - **Создать инсталляционный пакет для программы "Лаборатории Касперского"**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы "Лаборатории Касперского".
   - **Создать инсталляционный пакет для программы, указанной пользователем**. Выберите этот вариант, если вы хотите создать инсталляционный пакет для программы с помощью исполняемого файла. Как правило, исполняемый файл является установочным файлом программы.
     - **Копировать всю папку в инсталляционный пакет**
     - **Указать параметры установки**
   - **Выбрать программу из базы "Лаборатории Касперского" для создания инсталляционного пакета**. Выберите этот вариант, если вы хотите выбрать программу стороннего производителя из базы "Лаборатории Касперского", для которой требуется создать инсталляционный пакет. База данных создается автоматически при запуске задачи Загрузка обновлений в хранилище Сервера администрирования (на стр. 461); программы отображаются в списке.
   - **Создать инсталляционный пакет с образом операционной системы**. Выберите этот вариант, если вы хотите создать инсталляционный пакет с образом операционной системы эталонного устройства.

     В результате работы мастера создается задача Сервера администрирования с именем **Создание инсталляционного пакета на основе образа ОС эталонного устройства**. В результате выполнения этой задачи создается инсталляционный пакет, который можно использовать для развертывания образа операционной системы с помощью PXE-сервера или задачи удаленной установки.
4. Следуйте далее указаниям мастера.

В результате работы мастера создается инсталляционный пакет, который можно использовать для установки программы на клиентские устройства. Вы можете просмотреть инсталляционный пакет в папке **Инсталляционные пакеты** дерева консоли.

См. также:

Создание инсталляционного пакета ..... 372

## Выписка сертификата для инсталляционных пакетов программ

► *Чтобы выписать сертификат для инсталляционного пакета программы:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.
2. В контекстном меню папки **Инсталляционные пакеты** выберите пункт **Дополнительно**.

   В результате откроется окно свойств папки **Инсталляционные пакеты**.
3. В окне свойств папки **Инсталляционные пакеты** выберите раздел **Подпись автономных пакетов**.
4. В разделе **Подпись автономных пакетов** нажмите на кнопку **Задать**.

   Откроется окно **Сертификат**.
5. В поле **Тип сертификата** выберите открытый или закрытый тип сертификата:
   - Если выбрано значение **Контейнер PKCS#12**, укажите файл сертификата и пароль.
   - Если выбрано значение **X.509-сертификат**:
     a. укажите файл закрытого ключа (файл с расширением prk или pem);
     b. укажите пароль закрытого ключа;
     c. укажите файл открытого ключа (файл с расширением cer).
6. Нажмите на кнопку **ОК**.

В результате будет выписан сертификат для инсталляционного пакета программы.

## Установка программ на клиентские устройства

► *Чтобы установить программу на клиентские устройства:*

1. В дереве консоли в папке **Удаленная установка** по ссылке **Развернуть инсталляционный пакет на управляемые устройства (рабочие места)** запустите мастер развертывания защиты.
2. В окне мастера **Выбор инсталляционного пакета** укажите инсталляционный пакет программы, которую вы хотите установить.
3. Следуйте далее указаниям мастера.

В результате работы мастера создается задача удаленной установки программы на клиентских устройствах. Запустить или остановить задачу можно в папке **Задачи**.

Вы можете устанавливать Агент администрирования на клиентские устройства с операционными системами Windows, Linux и macOS с помощью мастера развертывания защиты.
Чтобы управлять 64-разрядными программами безопасности с помощью Kaspersky Security Center на устройствах с операционными системами Linux, необходимо использовать 64-разрядный Агент администрирования для Linux. Требуемую версию Агента администрирования можно загрузить с веб-сайта Службы технической поддержки https://support.kaspersky.com.
Перед выполнением удаленной установки Агента администрирования на устройство с операционной системой Linux необходимо подготовить устройство (на стр. 385).

# Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия.* Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- Серверы администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Описание**. В окне **Описание ревизии объекта** введите текст описания ревизии.

kaspersky

## В этом разделе



## О ревизиях объектов

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта (на стр. 813);
- просматривать выбранную ревизию (см. стр. 812);
- откатывать изменения объекта к выбранной ревизии (на стр. 815);
- сохранять ревизии в файле формата TXT (на стр. 815).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта (на стр. 815).

## Просмотр раздела История ревизий

Вы можете сравнить ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► *Чтобы просмотреть раздел **История ревизий** объекта:*

1. В дереве консоли выберите один из объектов:
   - узел **Сервер администрирования**;
   - папку **Политики**;
   - папку **Задачи**;
   - папку группы администрирования;

- папку **Учетные записи пользователей**;
- папку **Удаленные объекты**;
- папку **Инсталляционные пакеты**, вложенную в папку **Удаленная установка**.

2. В зависимости от местоположения соответствующего объекта выполните одно из следующих действий:
   - Если объект находится в узле **Сервер администрирования** или в папке группы администрирования, выберите пункт **Свойства** в контекстном меню объекта.
   - Если объект находится в папках **Политики**, **Задачи**, **Учетные записи пользователей**, **Удаленные объекты**, или **Инсталляционные пакеты**, выберите папку и в соответствующей рабочей области выберите объект.

   Откроется окно свойств объекта.
3. В окне свойств объекта выберите раздел **История ревизий**.

История ревизий отображается в рабочей области.

## Сравнение ревизий объекта

Вы можете сравнить предыдущие ревизии объекта с текущей ревизией, сравнить ревизии, выбранные в списке, или сравнить ревизию объекта с ревизией другого однотипного объекта.

► *Чтобы сравнить ревизии объекта:*

1. Выберите объект и перейдите к окну свойств этого объекта.
2. В окне свойств задачи выберите раздел **История ревизий** (на стр. 812).
3. В рабочей области в списке ревизий объекта выберите ревизию для сравнения.

   Для выбора более двух ревизий объекта используйте клавиши **SHIFT** и **CTRL**.
4. Выполните одно из следующих действий:
   - Нажмите на кнопку **Сравнить** и в раскрывающемся списке выберите одно из значений:
     - **Сравнить с текущей ревизией**

       Выберите этот вариант, чтобы сравнить выбранную ревизию с текущей.
     - **Сравнить выбранные ревизии**

       Выберите этот вариант, чтобы сравнить две выбранные ревизии.
     - **Сравнить с другой задачей**

       При работе с ревизиями задач выберите вариант **Сравнить с другой задачей**, чтобы сравнить выбранную ревизию с ревизией другой задачи.

       При работе с ревизиями политик выберите вариант **Сравнить с другой политикой**, чтобы сравнить выбранную ревизию с ревизией другой политики
   - Откройте окно свойств требуемой ревизии двойным щелчком мыши. В открывшемся окне свойств ревизии нажмите на одну из следующих кнопок:
     - **Сравнить с текущей ревизией**

       Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с текущей.

- **Сравнить с предыдущей**

  Нажмите на эту кнопку, чтобы сравнить выбранную ревизию с предыдущей.

Отчет о сравнении ревизий в формате HTML отображается в вашем браузере по умолчанию.

В отчете можно свернуть некоторые блоки параметров ревизии. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки (  ) рядом с названием блока.

В ревизии Сервера администрирования попадает информация об изменениях, кроме информации из следующих областей:

- раздела **Трафик**;
- раздела **Правила назначения тегов**;
- раздела **Уведомление**;
- раздела **Точки распространения**;
- раздела **Вирусная атака**.

  Из раздела **Вирусная атака** не будет записана информация о настройке активации политик по событию Вирусная атака.

Вы можете сравнивать ревизии удаленного объекта с ревизией существующего объекта, но не наоборот: вы не можете сравнивать ревизии существующего объекта с ревизией удаленного объекта.

## Установка срока хранения ревизий объектов и информации об удаленных объектах

Срок хранения ревизий объекта такой же, как срок хранения информации об удаленных объектах. Срок, заданный по умолчанию, – 90 дней. Этого достаточно для регулярного аудита программы.

Только пользователи с правами**Изменение** в области **Удаленные объекты** (на стр. 798) могут изменить срок хранения ревизий объектов и информации об удаленных объектах.

► *Чтобы изменить срок хранения ревизий объектов и информации об удаленных объектах:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно изменить срок хранения ревизий объектов и информации об удаленных объектах.
2. В контекстном меню объекта выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Хранение истории ревизий** укажите требуемый срок хранения (в днях).
4. Нажмите на кнопку **ОК**.

Ревизии объектов и информация об удаленных объектах будут храниться указанное количество дней.

## Просмотр ревизии объекта

Если вам понадобилось узнать, какие изменения проводились с объектом в определенный период, вы можете просмотреть ревизии объекта.

► *Чтобы просмотреть ревизии объекта:*

1. Перейдите к разделу **История ревизий** (на стр. 812) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно посмотреть.

3. Выполните одно из следующих действий:
   - Нажмите на кнопку **Посмотреть ревизию**.
   - Откройте окно свойств ревизии двойным щелчком мыши по названию ревизии и нажмите на кнопку **Посмотреть ревизию**.

   Отобразится отчет с параметрами выбранной ревизии объекта в формате HTML. В отчете можно свернуть некоторые блоки параметров ревизии объекта. Чтобы свернуть блок параметров ревизии, нажмите на значок стрелки ( ) рядом с названием блока.

## Сохранение ревизии объекта в файле

Вы можете сохранить ревизию объекта в текстовом файле, например, чтобы отправить файл по электронной почте.

► *Чтобы сохранить ревизию объекта в файле:*

1. Перейдите к разделу **История ревизий** (на стр. 812) объекта.
2. В списке ревизий объекта выберите ревизию, параметры которой нужно сохранить.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Сохранить в файл**.

Ревизия будет сохранена в файле формата TXT.

## Откат изменений

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► *Чтобы откатить изменения объекта:*

1. Перейдите к разделу **История ревизий** (на стр. 812) объекта.
2. В списке ревизий объекта выберите номер ревизии, к которой нужно откатить изменения.
3. Нажмите на кнопку **Дополнительно** и в раскрывающемся списке выберите значение **Откатить**.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

## Добавление описания ревизии

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии:*

1. Перейдите к разделу **История ревизий** (на стр. 812) объекта.
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Описание**.
4. В окне **Описание ревизии объекта** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.

5. Нажмите на кнопку **ОК**.

## Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы пользователей;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения (на стр. 814) информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** (на стр. 798) для области **Удаленные объекты**.

#### Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования программа перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные программы "Лаборатории Касперского" – Агент администрирования и программа безопасности, например Kaspersky Endpoint Security (если есть) – остаются на устройстве.

Kaspersky Security Center Cloud Console обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств (см. стр. 1126) и устройство соответствует критериям правила перемещения, устройство автоматически перемещается в группу администрирования в соответствии с правилом.
- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств (см. стр. 1063).

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически, вы можете сделать это только вручную. Если вам нужно удалить устройство с зашифрованным диском, сначала расшифруйте диск, а затем удалите устройство.
  При удалении устройства с зашифрованным диском данные, необходимые для расшифровки диска, также удаляются. В этом случае вы сможете расшифровать диск только в том случае, если у пользователя устройства есть пароль на расшифровку и на устройстве все еще установлена программа безопасности, которая использовалась для шифрования диска, например Kaspersky Endpoint Security для Windows.

При удалении устройства из группы Нераспределенные устройства вручную программа удаляет устройство из списка. После удаления устройства, установленные программы "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети (см. стр. 325), Kaspersky Security Center Cloud Console обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

### См. также:



### В этом разделе



## Удаление объекта

Вы можете удалять объекты, такие как политики, задачи, инсталляционные пакеты, внутренних пользователей и группы внутренних пользователей, если у вас есть права на изменение для категории Базовая функциональность (подробную информацию см. в разделе Назначение прав пользователям и группам пользователей) (на стр. 798).

► *Чтобы удалить объект:*

1. В рабочей области требуемой папки дерева консоли выберите объект.
2. Выполните одно из следующих действий:
   - В контекстном меню объекта выберите пункт **Удалить**.
   - Нажмите на кнопку **DELETE**.

Объект будет удален, и информация об этом будет записана в базу данных.

### См. также:



## Просмотр информации об удаленных объектах

Информация об удаленных объектах хранится в папке **Удаленные объекты** такой же срок, как и ревизии объекта (рекомендуемый срок составляет 90 дней).

Только пользователи с правами на **Чтение** для области **Удаленные объекты** могут просматривать список удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей (на стр. 798)).

► *Чтобы просмотреть список удаленных объектов,*

В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).

Если у вас нет прав на чтение для области **Удаленные объекты**, в папке **Удаленные объекты** будет отображаться пустой список.

В рабочей области папки **Удаленные объекты** содержится следующая информация об удаленных объектах:

- **Название**. Название удаленного объекта.
- **Тип**. Тип объекта, такой как политика, задача или инсталляционный пакет.
- **Время**. Время, когда объект был удален.
- **Пользователь**. Учетная запись пользователя, который удалил объект.

► *Чтобы просмотреть больше информации об удаленном объекте:*

1. В дереве консоли выберите пункт **Удаленные объекты** (по умолчанию папка **Удаленные объекты** вложена в папку **Дополнительно**).
2. В рабочей области папки **Удаленные объекты** выберите нужный объект.

   В правой части рабочей области отобразится поле для работы с выбранным объектом.
3. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в блоке работы с выбранным объектом.
   - В контекстном меню объекта выберите пункт **Свойства**.

   Откроется окно свойств объекта, в котором отображается следующая информация:
   - **Общие**
   - **История ревизий** (см. стр. 811)

## Удаление объектов из списка удаленных объектов

Только пользователи с правами **Изменение** для области **Удаленные объекты** могут удалять объекты из списка удаленных объектов (подобную информацию см. в разделе Назначение прав пользователям и группам пользователей (на стр. 798)).

► *Чтобы удалить объект из списка удаленных объектов:*

1. В дереве консоли выберите узел нужного Сервера администрирования и выберите папку **Удаленные объекты**.
2. В рабочей области папки выберите объект или объекты, которые вы хотите удалить.
3. Выполните одно из следующих действий:
   - Нажмите на кнопку **DELETE**.
   - В контекстном меню объекта или объектов, которые вы выбрали, выберите пункт **Удалить**.
4. В диалоговом окне нажмите на кнопку **Да**.

Объект удален из списка удаленных объектов. Вся информация объекта (включая все ревизии) удалена из базы данных. Вы не можете восстановить эту информацию.

kaspersky

# Хранилища данных

Этот раздел содержит информацию о данных, которые хранятся на Сервере администрирования и используются для отслеживания состояния клиентских устройств и для их обслуживания.

Данные, которые используются для отслеживания состояния устройств и их обслуживания, отображаются в папке дерева консоли **Хранилища**.

Папка **Хранилища** содержит следующие объекты:

- загруженные Сервером администрирования обновления, которые распространяются на клиентские устройства (на стр. 472);
- список оборудования, обнаруженного в сети;
- лицензионные ключи, обнаруженные на клиентских устройствах (на стр. 389);
- файлы, помещенные программами безопасности в карантинные папки на устройствах;
- файлы, помещенные в резервные хранилища устройств;
- файлы, для которых программы безопасности определили необходимость отложенной проверки.

## В этом разделе



## Экспорт списка объектов, находящихся в хранилище, в текстовый файл

Вы можете экспортировать в текстовый файл список объектов, находящихся в хранилище.

► *Чтобы экспортировать в текстовый файл список объектов, находящихся в хранилище:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку нужного вам хранилища.
2. В контекстном меню списка объектов хранилища выберите пункт **Экспортировать список**.

   В результате откроется окно **Экспорт списка**, в котором вы можете указать имя текстового файла и адрес папки, в которую он будет помещен.

## Инсталляционные пакеты

Kaspersky Security Center помещает в хранилища данных инсталляционные пакеты программ "Лаборатории Касперского" и программ сторонних производителей.

*Инсталляционный пакет* представляет собой набор файлов, необходимых для установки программы. Инсталляционный пакет содержит параметры процесса установки и первоначальной конфигурации устанавливаемой программы.

Если вы хотите установить какую-либо программу на клиентское устройство, для этой программы необходимо создать инсталляционный пакет (на стр. 809) или использовать уже созданный инсталляционный пакет. Список созданных инсталляционных пакетов содержится в папке дерева консоли **Удаленная установка**, во вложенной папке **Инсталляционные пакеты**.

### См. также:

Работа с инсталляционными пакетами .....371

## Основные статусы файлов в хранилище

Программы безопасности проверяют файлы на устройствах на наличие известных вирусов и других программ, представляющих угрозу, присваивают статусы файлам и помещают некоторые файлы в хранилище.

Например, программы безопасности могут:

- сохранять в хранилище копию файла перед удалением;
- изолировать в хранилище возможно зараженные файлы.

Основные статусы файлов приведены в таблице ниже. Вы можете получить более подробную информацию о действиях с файлами в справках программ безопасности.

*Таблица 72. Статусы файлов в хранилище*

| Название статуса | Описание статуса |
|---|---|
| Заражен | В файле найден участок кода известного вируса или другой представляющей угрозу программы, информация о которой содержится в антивирусных базах "Лаборатории Касперского". |
| Не заражен | В файле не обнаружено известных вирусов или других программ, представляющих угрозу. |
| Предупреждение. | В файле содержится участок кода, частично совпадающий с контрольным участком кода известной угрозы. |
| Возможно зараженный | В файле содержится либо модифицированный код известного вируса, либо код, напоминающий вирус, пока не известный "Лаборатории Касперского". |
| Помещен в папку пользователем | Пользователь самостоятельно поместил файл в хранилище, например, поведение файла давало основание подозревать в нем наличие угрозы. Пользователь может проверить файл на наличие в нем угроз с помощью обновленных баз. |
| Ложное срабатывание | Программа "Лаборатории Касперского" присвоила статус незараженному файлу как зараженному ввиду того, что его код напоминает код вируса. После проверки с применением обновленных баз файл определяется как незараженный. |
| Вылечен | Файл удалось вылечить. |
| Удален | Файл удален в результате обработки. |
| Защищен паролем | Файл не может быть обработан по причине того, что он защищен паролем. |

kaspersky

## См. также:

Значки статусов файлов в Консоли администрирования .....905

## Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования Kaspersky Security Center. Эта информация хранится в виде списка в папке **Срабатывание правил в интеллектуальном режиме**, которая вложена в папку **Хранилища**. Вы можете подтвердить обнаружение как корректное (на стр. 821) или добавить его в исключения (на стр. 823), после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий (на стр. 1376) на Сервере администрирования (вместе с остальными событиями) и в отчете (на стр. 1368) Адаптивный контроль аномалий.

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

## В этом разделе

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий821

Добавление исключений в правила Адаптивного контроля аномалий.....823

## Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

► *Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Статус**

     **Исключение** – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена

синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

**Подтверждение** – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

Пусто – если администратор не обработал обнаружение.

- **Количество срабатываний для всех правил**

  Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного процесса**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA-256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA-256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA-256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA-256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработан**

  Дата обнаружения аномалии.

► *Чтобы просмотреть свойства каждого элемента:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно → Хранилища**).
3. В рабочей области папки **Срабатывание правил в статусе Интеллектуальное обучение** выберите требуемый объект.
4. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
   - В контекстном меню объекта выберите пункт **Свойства**.

   В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения (на стр. 821) любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий.

► *Чтобы подтвердить объект,*

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждение**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

► *Чтобы добавить объект в исключения,*

в списке обнаруженных объектов в контекстном меню одного или нескольких объектов выберите пункт **Добавить в исключения**.

В результате запустится мастер добавления исключений (на стр. 823). Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

## Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

► *Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно → Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

В результате запустится мастер добавления исключений.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте закладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений**.

### В этом разделе



*Шаг 1. Выбор программы*

Этот шаг можно пропустить, если у вас есть только программа Kaspersky Endpoint Security для Windows и нет других программ, поддерживающих правила Адаптивного контроля аномалий.

Мастер добавления исключений отображает список программ "Лаборатории Касперского", для которых плагины управления позволяют добавлять исключения к политикам для этих программ. Выберите программу из списка и нажмите на кнопку **Далее**, чтобы продолжить выбор политики, для которой будет добавлено исключение.

*Шаг 2. Выбор политики (политик)*

Мастер отображает список политик (с профилями политик) для Kaspersky Endpoint Security.

Выберите все политики и профили политик, в которые вы хотите добавить исключения, и нажмите на кнопку **Далее**.

*Шаг 3. Обработка политики (политик)*

Мастер отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

Это последний шаг мастера. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

## Карантин и резервное хранилище

Антивирусные программы "Лаборатории Касперского", установленные на клиентских устройствах, в процессе проверки устройств могут помещать файлы на карантин или в резервное хранилище.

*Карантин* – это специальное хранилище, в которое помещаются файлы, возможно зараженные вирусами или неизлечимые на момент обнаружения.

*Резервное хранилище* предназначено для хранения резервных копий файлов, которые были удалены или изменены в процессе лечения.

Kaspersky Security Center формирует общий список файлов, помещенных на карантин и в резервное хранилище программами "Лаборатории Касперского" на устройствах. Агенты администрирования клиентских устройств передают информацию о файлах на карантине и в резервных хранилищах на Сервер администрирования. Через Консоль администрирования можно просматривать свойства файлов, находящихся в хранилищах на устройствах, запускать проверку вредоносного ПО хранилищ и удалять из них файлы. Значки статусов файлов описаны в приложении (на стр. 905).

Работа с карантином и резервным хранилищем доступна для Антивируса Касперского для Windows Workstations и Антивируса Касперского для Windows Servers версий 6.0 и выше, а также для Kaspersky Endpoint Security 10 для Windows и выше.

Kaspersky Security Center не копирует файлы из хранилищ на Сервер администрирования. Все файлы размещаются в хранилищах на устройствах. Восстановление файлов выполняется на устройстве, где установлена программа безопасности, поместившая файл в хранилище.

## В этом разделе



## Включение удаленного управления файлами в хранилищах

По умолчанию удаленное управление файлами в хранилищах на клиентских устройствах отключено.

► *Чтобы включить удаленное управление файлами в хранилищах на клиентских устройствах:*

1. В дереве консоли выберите группу администрирования, для которой требуется включить удаленное управление файлами хранилищ.
2. В рабочей области группы откройте закладку **Политики**.
3. На закладке **Политики** выберите политику программы безопасности, помещающей файлы в хранилища на устройствах.
4. В окне свойств политики в блоке **Информировать Сервер администрирования** установите флажки, соответствующие хранилищам, для которых вы хотите включить удаленное управление.

   Расположение блока **Информировать Сервер администрирования** в окне свойств политики и названия флажков в блоке индивидуальны для каждой программы безопасности.

## Просмотр свойств файла, помещенного в хранилище

► *Чтобы просмотреть свойства файла, помещенного на карантин или в резервное хранилище:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, параметры которого требуется просмотреть.
3. В контекстном меню файла выберите пункт **Свойства**.

## Удаление файлов из хранилища

► *Чтобы удалить файл, помещенный на карантин или в резервное хранилище:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Удалить**.
   - По ссылке **Удалить объекты** (**Удалить объект**) при удалении одного файла в блоке работы с выбранными файлами.

В результате программы безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удалят файлы из этих хранилищ.

## Восстановление файлов из хранилища

► *Чтобы восстановить файл из карантина или резервного хранилища:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) с помощью клавиш **Shift** и **Ctrl** выберите файлы, которые требуется восстановить.
3. Запустите процесс восстановления файлов одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Восстановить**.
   - По ссылке **Восстановить** в блоке работы с выбранными файлами.

В результате программы безопасности, поместившие файлы в хранилища на клиентских устройствах, восстановят файлы в исходные папки.

## Сохранение файла из хранилища на диск

Kaspersky Security Center позволяет сохранять на диск копии файлов, помещенных программой безопасности на карантин или в резервное хранилище на клиентском устройстве. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку.

► *Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или **Резервное хранилище**.
2. В рабочей области папки **Карантин** (**Резервное хранилище**) выберите файл, который требуется скопировать на жесткий диск.
3. Запустите процесс копирования файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате программа безопасности, поместившая файл на карантин на клиентском устройстве, сохранит копию файла в указанную папку.

### Сканирование файлов, находящихся на карантине

► *Чтобы проверить файлы, находящиеся на карантине:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Карантин** или Резервное хранилище.
2. В рабочей области папки **Карантин** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется проверить.
3. Запустите процесс проверки файлов одним из следующих способов:
   - В контекстном меню файла выберите пункт **Проверить**.
   - По ссылке **Проверить** в блоке работы с выбранными файлами.

   Приложение запускает задачу проверки по требованию для приложений безопасности, которые поместили выбранные файлы на карантин, на устройствах, где хранятся эти файлы.

## Активные угрозы

Информация о необработанных файлах, обнаруженных на клиентских устройствах, содержится в папке **Хранилища**, во вложенной папке **Активные угрозы**.

Отложенная обработка и дезинфекция выполняются программой безопасности по запросу или после определенного события. Вы можете настраивать параметры отложенного лечения файлов.

### В этом разделе



### Дезинфекция необработанного файла

► *Чтобы запустить лечение необработанного файла:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.

2. В рабочей области папки **Активные угрозы** выберите файл, который требуется вылечить.
3. Запустите процесс лечения файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Лечить**.
   - По ссылке **Лечить** в блоке работы с выбранным файлом.

   В результате выполняется попытка лечения файла.

Если файл вылечен, программа безопасности, установленная на клиентском устройстве, восстанавливает его в исходную папку. Запись о файле удаляется из списка папки **Активные угрозы**. Если лечение файла невозможно, программа безопасности, установленная на устройстве, удаляет файл с устройства. Запись о файле удаляется из списка папки **Активные угрозы**.

## Сохранение необработанного файла на диск

Kaspersky Security Center позволяет сохранять на диск копии необработанных файлов, обнаруженные на клиентских устройствах. Файлы копируются на устройство, на котором установлен Kaspersky Security Center, в указанную вами папку. Вы можете загрузить файл только в том случае, если файл хранится в хранилище резервных копий управляемого устройства https://support.kaspersky.com/KESWin/11.5.0/ru-RU/178491.htm.

► *Чтобы сохранить копию необработанного файла на диск:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** выберите файлы, которые требуется скопировать на диск.
3. Запустите процесс копирования файла одним из следующих способов:
   - В контекстном меню файла выберите пункт **Сохранить на диск**.
   - В блоке работы с выбранным файлом нажмите на ссылку **Сохранить на диск**.

В результате программа безопасности клиентского устройства, на котором обнаружен выбранный необработанный файл, сохранит копию файла в указанную папку.

## Удаление файлов из папки "Активные угрозы"

► *Чтобы удалить файл из папки **Активные угрозы**:*

1. В дереве консоли в папке **Хранилища** выберите вложенную папку **Активные угрозы**.
2. В рабочей области папки **Активные угрозы** с помощью клавиш **SHIFT** и **CTRL** выберите файлы, которые требуется удалить.
3. Удалите файлы одним из следующих способов:
   - В контекстном меню файлов выберите пункт **Удалить**.
   - По ссылке **Удалить объекты** (**Удалить объект**) при удалении одного файла в блоке работы с выбранными файлами.

   В результате программы безопасности, поместившие выбранные файлы в хранилища на клиентских устройствах, удаляют файлы из этих хранилищ. Записи о файлах удаляются из списка в папке **Активные угрозы**.

kaspersky

# Kaspersky Security Network и Kaspersky Private Security Network

В безопасном состоянии используется только Локальный KSN (KPSN). Использование Глобального KSN ведет к выходу программы из безопасного состояния.

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

## В этом разделе



## О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о программах, установленных на управляемых устройствах.

Kaspersky Security Center поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе программ "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN (см. стр. 830). Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Kaspersky Security Center использует это решение по умолчанию.
- *Локальный KSN* – это решение, которое предоставляет пользователям устройств с установленными программами "Лаборатории Касперского" доступ к базам данных Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в KSN. Kaspersky Private Security Network (Локальный KSN) предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

- Устройства пользователей не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

Вы можете настроить параметры доступа (см. стр. 830) Kaspersky Private Security Network в разделе **Параметры KSN прокси-сервера** окна свойств Сервера администрирования.

Программа предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. стр. 832).

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871). Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Параметры прокси-сервер KSN** окна свойств Сервера администрирования (см. стр. 830).

## Настройка доступа к Kaspersky Security Network

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

► *Чтобы настроить доступ Сервера администрирования к Kaspersky Security Network (KSN):*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить доступ к KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Прокси-сервер KSN** → **Параметры прокси-сервера KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы использовать службу прокси-сервера KSN.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

5. Включите параметр **Я принимаю условия использования Kaspersky Security Network**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете Локальный KSN, включите параметр **Настроить Локальный KSN** и нажмите на кнопку **Файл с параметрами прокси-сервера KSN**, чтобы загрузить параметры Локального KSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами Локального KSN.

   При включении Локального KSN обратите внимание на точки распространения настроенные на отправление KSN запросов напрямую облачной-службе KSN. Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к облачной-службе KSN. Чтобы перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения. Вы можете включить этот параметр в свойствах точки распространения или политики Агента администрирования.

   Когда вы устанавливаете флажок **Настроить Локальный KSN**, появляется сообщение с информацией о Локальном KSN.

   Работу с Локальным KSN поддерживают следующие программы "Лаборатории Касперского":

   - Kaspersky Security Center;
   - Kaspersky Endpoint Security для Windows;
   - Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2;
   - Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент.

   Если вы включите опцию **Настроить Локальный KSN** в Kaspersky Security Center, эти программы получат об этом информацию о поддержке Локального KSN. В окне свойств программы в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается **Поставщик KSN: Локальный KSN**. В противном случае отображается **Поставщик KSN: Глобальный KSN**.

   Если для работы с Локальным KSN вы используете версии программ ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование Локального KSN.
   Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен Локальный KSN в окне свойств Сервера администрирования в разделе **Прокси-сервер KSN → Параметры прокси-сервера KSN**.

   Установите флажок **Игнорировать параметры прокси-сервера для подключения к Локальному KSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали Локальный KSN напрямую. В противном случае запрос от управляемой программы не будет передан в Локальный KSN.

6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:

   - В блоке **Параметры подключения**, в поле ввода **TCP-порт** укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.

- Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

7. Включите параметр **Подключать подчиненные Серверы администрирования к KSN через главный Сервер**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен, подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

   > Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Прокси-сервер KSN** также установлен флажок **Использовать Сервер администрирования как прокси-сервер**.

8. Нажмите на кнопку **ОК**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

► *Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):*

1. Убедитесь, что точка распространения была назначена вручную (см. стр. 481).
2. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
3. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
4. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.
5. Выберите в списке точку распространения и по кнопке **Свойства** откройте окно ее свойств.
6. В окне свойств точки распространения в разделе **Прокси-сервер KSN** выберите **Доступ к облачной службе KSN непосредственно через интернет**.
7. Нажмите на кнопку **ОК**.

Точка распространения будет исполнять роль прокси-сервера KSN.

## Включение и отключение KSN

► *Чтобы включить KSN:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервер KSN**.
4. Установите флажок **Использовать Сервер администрирования как прокси-сервер**.

В результате будет включена служба прокси-сервера KSN.

5. Установите флажок **Я принимаю условия использования Kaspersky Security Network**.

   В результате KSN будет включен.

   Если флажок установлен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". Установив флажок, вы должны прочитать и принять условия Положения о KSN.

6. Нажмите на кнопку **ОК**.

► *Чтобы выключить KSN:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно включить KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервер KSN**.
4. Снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN, или снимите флажок **Я принимаю условия использования Kaspersky Security Network**.

   Если флажок снят, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

   Если вы используете Локальный KSN, снимите флажок **Настроить Локальный KSN**.

   В результате KSN будет выключен.

5. Нажмите на кнопку **ОК**.

## Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вы должны прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

► *Чтобы просмотреть принятое Положение о KSN:*

1. В дереве консоли выберите Сервер администрирования, для которого включен KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите подраздел **Параметры прокси-сервер KSN**.
4. Перейдите по ссылке **Просмотреть Положение о KSN**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

## Просмотр статистики прокси-сервера KSN

*Прокси-сервер KSN* – это служба, обеспечивающая взаимодействие между инфраструктурой Kaspersky Security Network и клиентскими устройствами, находящимися под управлением Сервера администрирования.

Использование прокси-сервера KSN предоставляет вам следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.

- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

В окне свойств Сервера администрирования вы можете настроить параметры прокси-сервера KSN и просмотреть статистическую информацию об использовании прокси-сервера KSN.

► *Чтобы просмотреть статистику работы прокси-сервера KSN:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно просмотреть статистику KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Статистика прокси-сервера KSN**.

   В разделе отображается статистика работы прокси-сервера KSN. Если необходимо, выполните дополнительные действия:

   - по кнопке **Обновить** обновите статистическую информацию об использовании прокси-сервера KSN;
   - по кнопке **Экспортировать в файл** экспортируйте данные статистики в файл формата CSV;
   - по кнопке **Проверить подключение к KSN** проверьте, подключен ли Сервер администрирования к KSN в настоящий момент.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

## Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN (на стр. 833), которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования или после обновления с предыдущей версии Сервера администрирования, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

► *Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:*

1. В дереве консоли выберите узел **Сервер администрирования – <Имя Сервера>**.
2. На закладке **Мониторинг** в разделе **Мониторинг** перейдите по ссылке **Принятое Положение о Kaspersky Security Network устарело**.

   Откроется окно **Положение о KSN**.
3. Внимательно прочтите Положение о KSN, а затем примите решение. Если вы принимаете условия обновленного Положения о KSN, нажмите на кнопку **Я принимаю условия Лицензионного соглашения**. Если вы отклоняете условия обновленного Положения о KSN, нажмите на кнопку **Отмена**.

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN (на стр. 833) в свойствах Сервера администрирования.

kaspersky

### Дополнительная защита с использованием Kaspersky Security Network

"Лаборатория Касперского" предоставляет дополнительный уровень защиты с использованием Kaspersky Security Network. Этот способ защиты нацелен на эффективную борьбу против постоянных угроз повышенной сложности и угроз нулевого дня. Объединенные с Kaspersky Endpoint Security облачные технологии и экспертные знания вирусных аналитиков "Лаборатории Касперского" обеспечивают мощную защиту против сложнейших угроз в сети.

Более подробную информацию о дополнительной защите в Kaspersky Endpoint Security вы можете найти на веб-сайте "Лаборатории Касперского".

### Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

► *Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:*

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все программы** → **Администрирование** → **Службы**).
2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

► *Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:*

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.
2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

## Переключение между онлайн-справкой и офлайн-справкой

Если у вас нет доступа в интернет, вы можете использовать офлайн-справку.

► *Чтобы переключиться между онлайн-справкой и офлайн-справкой:*

1. В главном окне программы Kaspersky Security Center выберите в дереве консоли узел **Kaspersky Security Center**.
2. Перейдите по ссылке **Параметры общего интерфейса**.

   Откроется окно параметров.
3. В окне свойств нажмите на ссылку **Использовать офлайн-справку**.
4. Нажмите на кнопку **ОК**.

Параметры применены и сохранены. Вы можете в любой момент изменить параметры и начать пользоваться онлайн-справкой в любое время.

# Экспорт событий в SIEM-системы

В этом разделе описана процедура экспорта событий, зарегистрированных в Kaspersky Security Center, во внешние системы управления событиями информационной безопасности (SIEM-системы, Security Information and Event Management).

## См. также:



## В этом разделе



## Сценарий: Настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

**Предварительные требования**

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий (см. стр. 839).
- Убедитесь, что у вас есть значения системных параметров (см. стр. 838).

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- Настройка SIEM-системы для получения событий из Kaspersky Security Center

  Инструкции: Настройка экспорта событий в SIEM-системе (см. стр. 841).
- Выбор события, которые вы хотите экспортировать в SIEM-систему:

  Инструкции:

  Консоль администрирования: Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog (см. стр. 843), Выбор общих событий для экспорта в формате Syslog (см. стр. 845).

  Kaspersky Security Center 14.2 Web Console: Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog (см. стр. 1385), Выбор общих событий для экспорта в формате Syslog (см. стр. 1386).
- Настройка экспорта событий в SIEM-систему одним из следующих способов:

  Укажите протоколы TCP/IP, UDP или TLS over TCP.

  Инструкции:

  Консоль администрирования: Настройка экспорта событий в SIEM-системы (см. стр. 847).

  Kaspersky Security Center 14.2 Web Console: Настройка экспорта событий в SIEM-системы (см. стр. 1388).

  Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

**Результаты**

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта (см. стр. 851), если вы выбрали события, которые хотите экспортировать.

## См. также:

## Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

  **Протокол**Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

### См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Вы можете экспортировать эту информацию во внешние SIEM-системы (см. стр 836). Экспорт информации о событиях во внешние SIEM-системы позволяет администраторам SIEM-систем оперативно реагировать на события системы безопасности, произошедшие на управляемых устройствах или группах устройств.

#### Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых программах "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых программ "Лаборатории Касперского". Каждая управляемая программа "Лаборатории Касперского" имеет собственный набор событий.

#### События источников

События могут генерироваться следующими программами:

- Компоненты программы Kaspersky Security Center:
  - Сервер администрирования (см. стр. 619);
  - Агент администрирования (см. стр. 644);

  - Сервер iOS MDM;
  - Сервер мобильных устройств Exchange ActiveSync.
- Управляемые программы "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми программами "Лаборатории Касперского", см. в документации соответствующей программы.

Просмотреть полный список событий, которые может генерировать программа, можно на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

**Уровень важности событий**

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

### См. также:


События компонентов Kaspersky Security Center ..... 618

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog ..... 843

Выбор общих событий для экспорта в формате Syslog ..... 845


## Об экспорте событий

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ

связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

**Способы отправки событий из Kaspersky Security Center**

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в программах "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования (см. стр. 843) или Kaspersky Security Center 14.2 Web Console (см. стр. 1386). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

  Протоколы CEF и LEEF можно использовать для экспорта общих событий (на стр. 838). При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

  > Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного лицензионного ключа (на стр. 389).

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

**Получение событий SIEM-системой**

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

kaspersky

См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

# О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

### Настройка приемника сообщений

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

  Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

  Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

  Протокол, используемый для экспорта событий в SIEM-систему. Это может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.

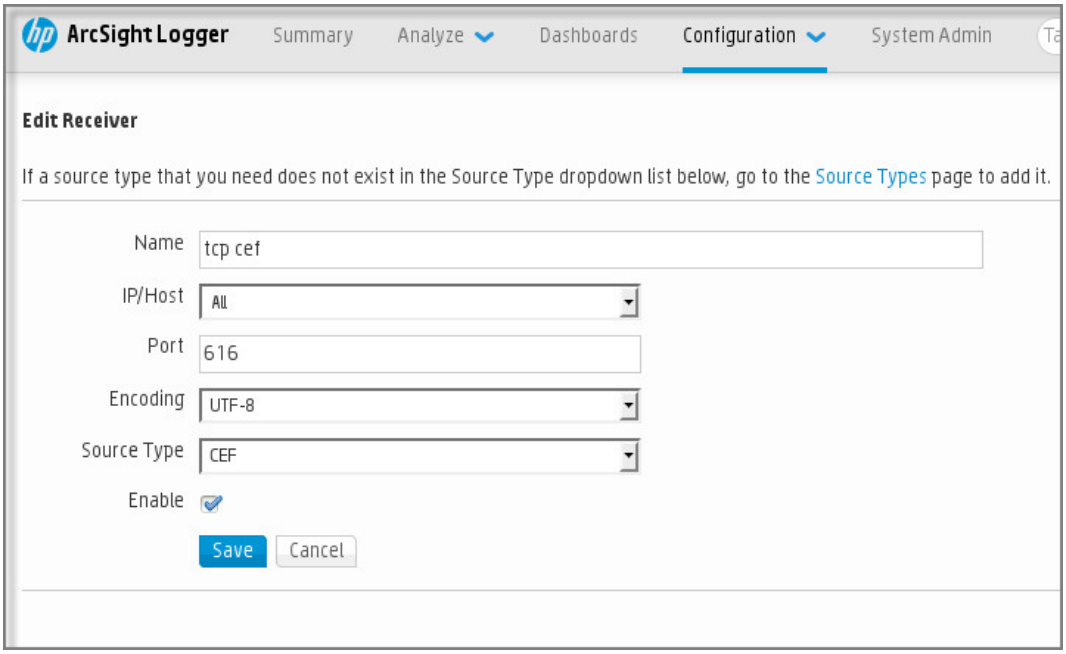



Figure 6. Пример настройки приемника сообщений

**Анализатор сообщений**

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

В каждой SIEM-системе имеется набор стандартных анализаторов сообщений. "Лаборатория Касперского" также предоставляет анализаторы сообщений для некоторых SIEM-систем, например, для QRadar и ArcSight. Вы можете загрузить эти анализаторы сообщений с веб-страниц соответствующих SIEM-систем. При настройке приемника можно выбрать используемый анализатор сообщений: один из стандартных анализаторов вашей SIEM-системы или анализатор, предоставляемый "Лабораторией Касперского".

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

# Выбор событий для экспорта в SIEM-системы в формате Syslog

В этом разделе описывается, как выбрать события для дальнейшего экспорта в SIEM-системы в формате Syslog.

kaspersky

## См. также:



## В этом разделе



## О выборе событий для экспорта в SIEM-систему в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.
- Выбор событий для управляемой программы. Если вы выбираете экспортируемые события для управляемой программы, установленной на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

## См. также:



## Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в отдельной управляемой программе, установленной на управляемом устройстве, выберите для программы события для экспорта. В случае, если ранее экспортируемые события были выбраны в политике, вам не удастся переопределить выбранные события для отдельной программы, управляемой этой политикой.

► *Чтобы выбрать события для отдельной управляемой программы:*

1. В дереве консоли Kaspersky Security Center выберите узел **Управляемые устройства** и перейдите на закладку **Устройства**.
2. Откройте контекстное меню требуемого устройства по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств устройства выберите раздел **Программы**.
4. В появившемся списке программ выберите программу, события которой требуется экспортировать, и нажмите на кнопку **Свойства**.
5. В окне свойств программы выберите раздел **Настройка событий**.

6. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.
7. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog. Выключите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.

Если свойства события заданы в политике, поля этого окна недоступны для редактирования.

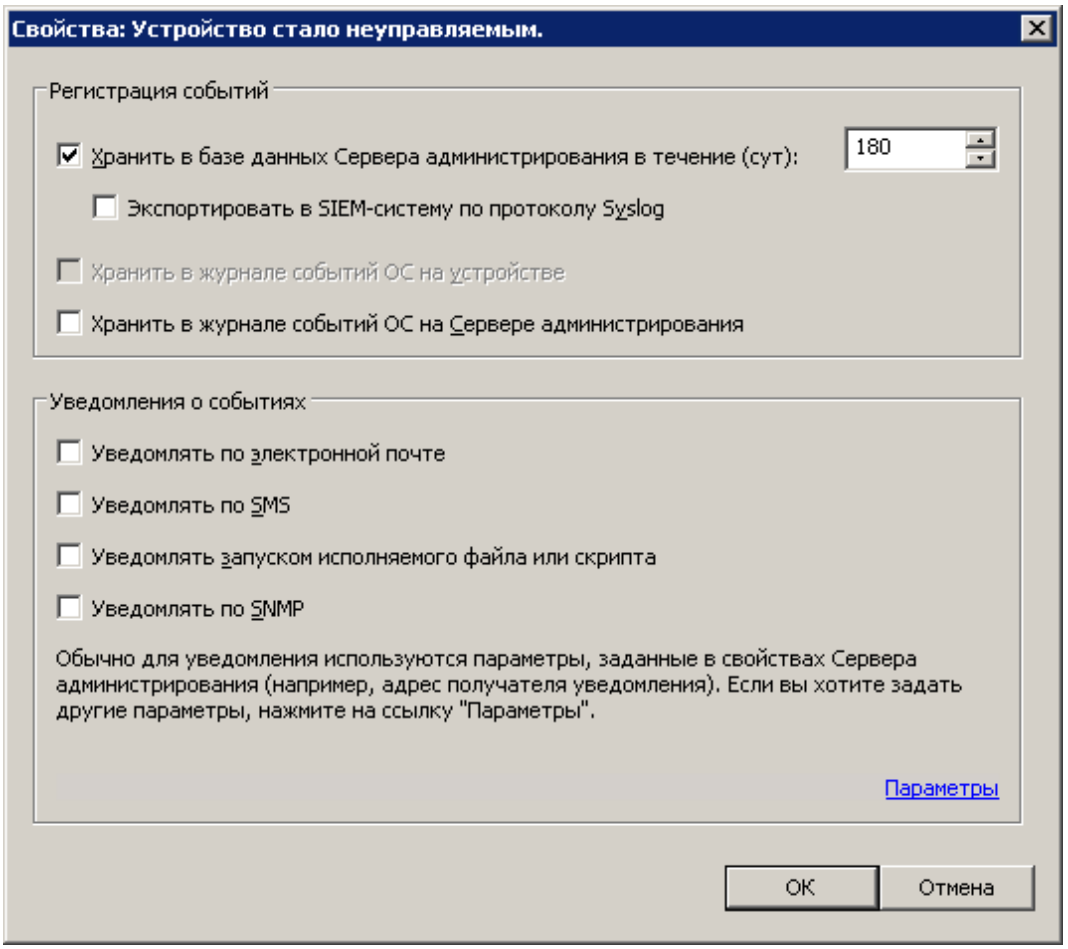



Figure 7. Окно свойств событий

8. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
9. Нажмите на кнопку **ОК** в окне свойств программы и в окне свойств устройства.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

## См. также

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Выбор общих событий для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших во всех программах, управляемых определенной политикой, выберите экспортируемые события в политике. В этом случае вы не можете выбрать события для отдельной управляемой программы.

► *Чтобы выбрать общие события для экспорта в SIEM-систему:*

1. В дереве консоли Kaspersky Security Center выберите узел **Политики**.
2. Откройте контекстное меню требуемой политики по правой клавише мыши и выберите пункт **Свойства**.
3. В открывшемся окне свойств политики выберите раздел **Настройка событий**.
4. В появившемся списке событий выберите одно или несколько событий, которые требуется экспортировать в SIEM-систему, и нажмите на кнопку **Свойства**.

   Если требуется выбрать все события, нажмите на кнопку **Выбрать все**.
5. В открывшемся окне свойств событий выберите параметр **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отметить выбранные события для экспорта в формате Syslog. Снимите флажок **Экспортировать в SIEM-систему по протоколу Syslog**, чтобы отменить выбор событий для экспорта в формате Syslog.

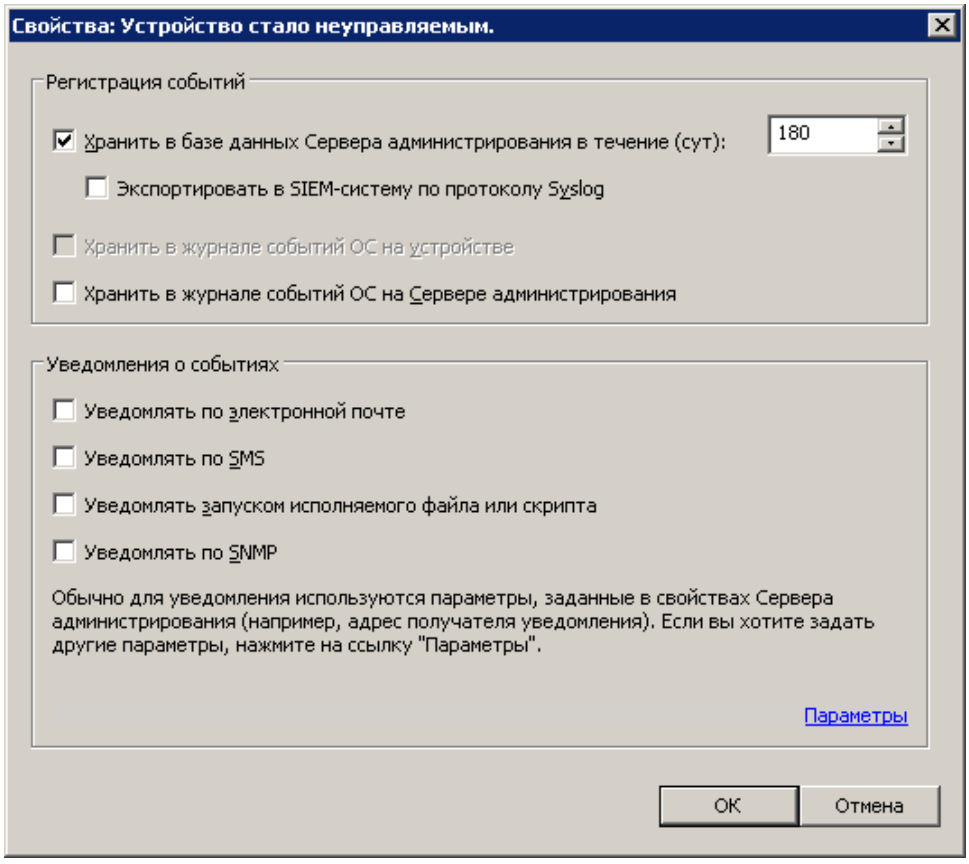



Figure 8. Окно свойств событий

6. Нажмите на кнопку **ОК**, чтобы сохранить изменения.
7. В окне свойств политики нажмите на кнопку **ОК**.

Выбранные события будут отправляться в SIEM-систему в формате Syslog. События, выбор которых вы отменили параметром **Экспортировать в SIEM-систему по протоколу Syslog**, не будут экспортироваться в SIEM-систему. Экспорт начнется сразу после того, как вы включите автоматический экспорт и выберете экспортируемые события. Выполните настройку SIEM-системы, чтобы обеспечить получение событий из Kaspersky Security Center.

### См. также

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 (https://tools.ietf.org/html/rfc5424) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

### См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (на стр. 838), а также событий, переданных программами "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует.

Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного лицензионного ключа (на стр. 389).

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

*Таблица 73. Форматы экспорта событий в SIEM-систему*

| SIEM-система | Формат экспорта |
|---|---|
| QRadar | LEEF |
| ArcSight | CEF |
| Splunk | CEF |

- LEEF – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

См. также:

Сценарий: Настройка экспорта событий в SIEM-системы .....836

# Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Вы можете включить автоматический экспорт событий в Kaspersky Security Center.

Только общие события (на стр. 838) могут быть экспортированы от управляемых программ в формате CEF и LEEF. Специфические события программ (на стр. 838) не могут быть экспортированы от управляемых программ в формате CEF и LEEF. Если необходимо экспортировать события управляемых программ или пользовательский набор событий, который настроен с помощью политик управляемых программ, используйте экспорт событий в формате Syslog.

► *Чтобы включить автоматический экспорт общих событий:*

1. В дереве консоли Kaspersky Security Center выберите узел с именем Сервера администрирования, события которого необходимо экспортировать.

2. В рабочей области выбранного Сервера администрирования перейдите на закладку **События**.
3. Нажмите на стрелку рядом со ссылкой **Настроить параметры уведомлений и экспорта событий** и в раскрывающемся списке выберите значение **Настроить экспорт в SIEM-систему**.

   Откроется окно свойств событий на разделе **Экспорт событий**.
4. В разделе **Экспорт событий** укажите следующие параметры:

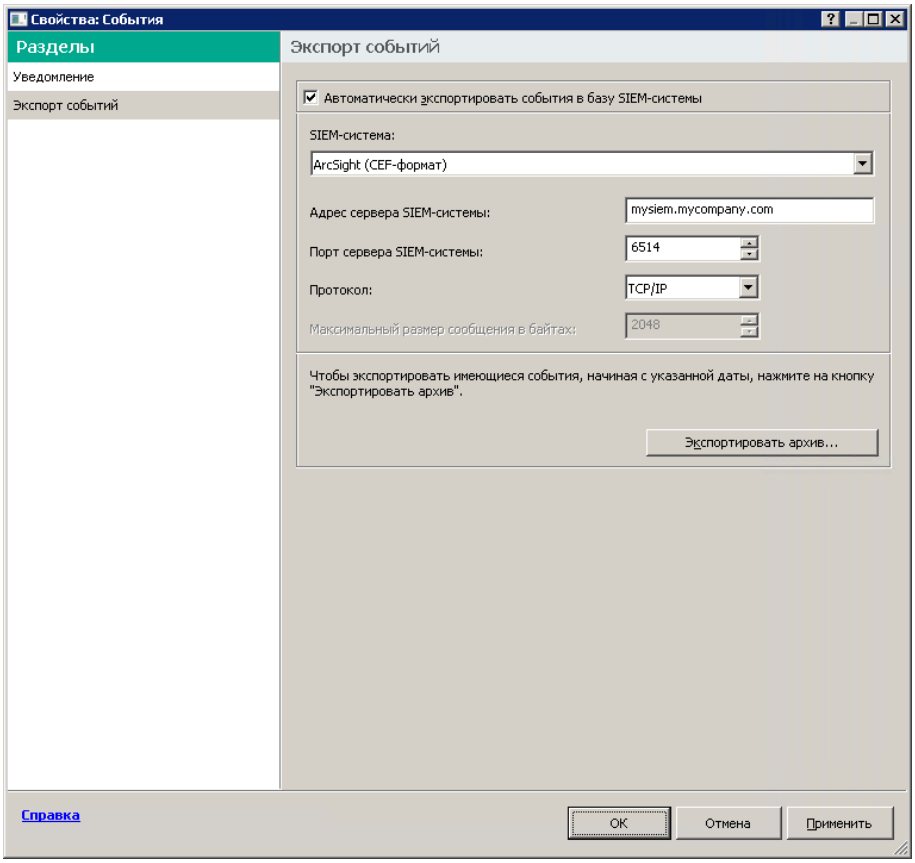



Figure 9. Раздел Экспорт событий

- **Автоматически экспортировать события в базу SIEM-системы**

  Установите этот флажок, для того чтобы включить автоматический экспорт событий в SIEM-систему. При установке этого флажка все поля в разделе **Экспорт событий** становятся доступными для редактирования.
- **SIEM-система**

  Выберите, в какую SIEM-систему будет выполняться экспорт событий: QRadar® (LEEF-формат), ArcSight (CEF-формат), Splunk® (CEF-формат) и формат Syslog (RFC 5424).
- **Адрес сервера SIEM-системы**

  Укажите адрес сервера SIEM-системы. Адрес сервера можно указать в формате DNS- или NetBIOS-имени или IP-адреса.
- **Порт сервера SIEM-системы**

Укажите номер порта для соединения с сервером SIEM-системы. Этот номер порта должен совпадать с номером порта, который вы указываете в настройках приемника SIEM-системы для получения событий (см. стр. 850).

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## В этом разделе



## Создание SQL-запроса с помощью утилиты klsql2

В этом разделе приведены инструкции по загрузке и использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты.

► *Чтобы загрузить и использовать утилиту klsql2:*

1. Загрузите утилиту klsql2 (https://media.kaspersky.com/utilities/CorporateUtilities/klsql2.zip) с веб-сайта "Лаборатории Касперского". Не используйте версии утилиты klsql2, предназначенные для старых версий Kaspersky Security Center.
2. Скопируйте и извлеките содержимое архива klsql2.zip в любую папку на устройстве, на котором установлен Сервер администрирования Kaspersky Security Center.

   Пакет klsql2.zip содержит следующие файлы:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Откройте файл src.sql с помощью любого текстового редактора.
4. В файле src.sql введите требуемый SQL-запрос и сохраните файл.
5. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

   ```
   klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.
6. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.
7. Откройте созданный файл result.xml и посмотрите результаты выполнения SQL-запроса.

Вы можете редактировать файл src.sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

## См. также

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

**Пример:**

```
SELECT
e.nId,                                  /* идентификатор события
*/
e.tmRiseTime,                           /* время возникновения
события */
e.strEventType,                         /* внутреннее имя типа
события */
e.wstrEventTypeDisplayName,             /* отображаемое имя
события */
e.wstrDescription,                      /* отображаемое описание
события */
e.wstrGroupName,                    /* имя группы устройств */
h.wstrDisplayName,                      /* отображаемое имя
устройства, на котором произошло событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp      /*          IP-адрес
устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

### См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Просмотр имени базы данных Kaspersky Security Center

Может быть полезно знать имя базы данных, если вам нужно, например, отправить SQL-запрос и подключиться к базе данных из редактора скриптов SQL.

► *Чтобы просмотреть имя базы данных Kaspersky Security Center:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В появившемся окне свойств Сервера администрирования выберите пункт **Дополнительно**, а затем **Информация об используемой базе данных**.
3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных (см. рис. ниже):

- **Имя экземпляра**

  Имя экземпляра используемой базы данных Kaspersky Security Center. Значение по умолчанию – *.\KAV_CS_ADMIN_KIT.*

- **Имя базы данных**

  Имя базы данных SQL Kaspersky Security Center. По умолчанию указано значение *KAV*.

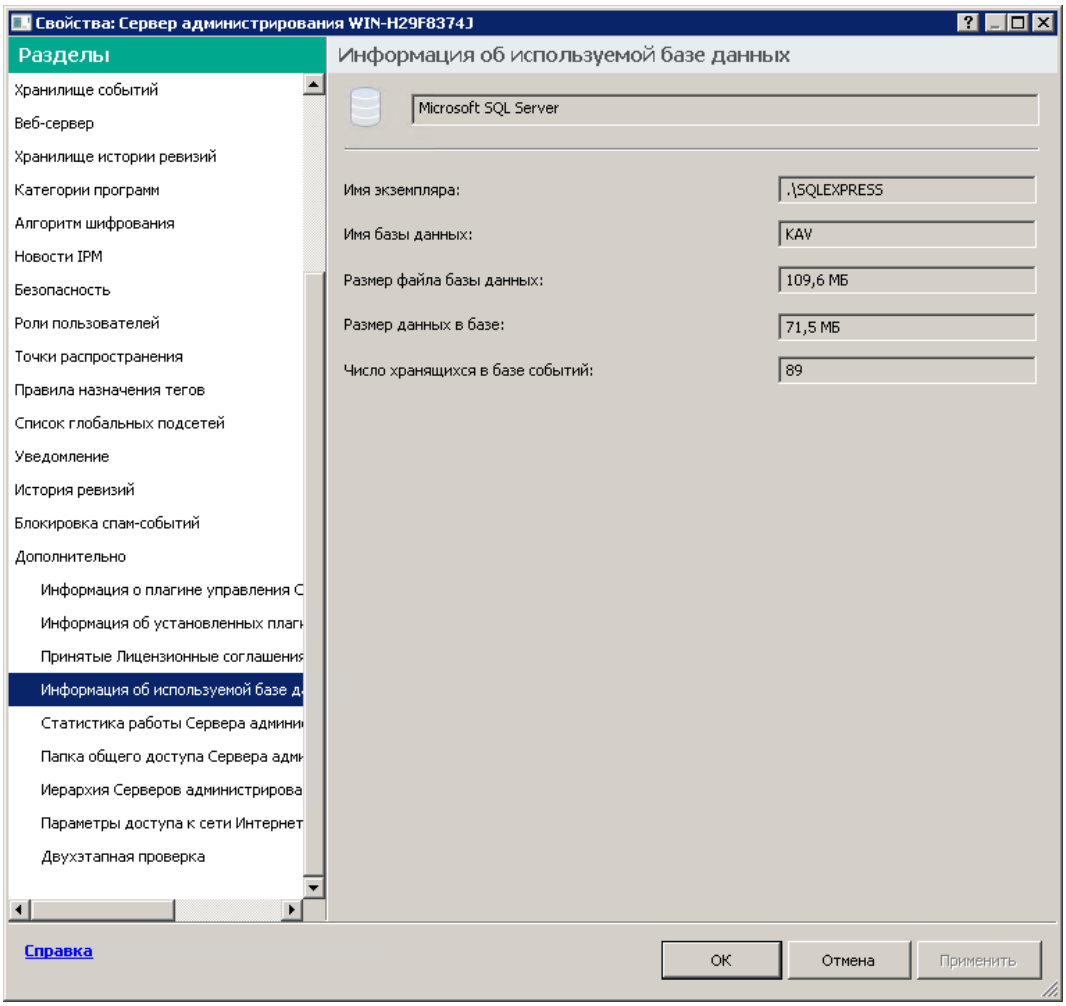



Figure 10. Имя базы данных SQL Kaspersky Security Center

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

# Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

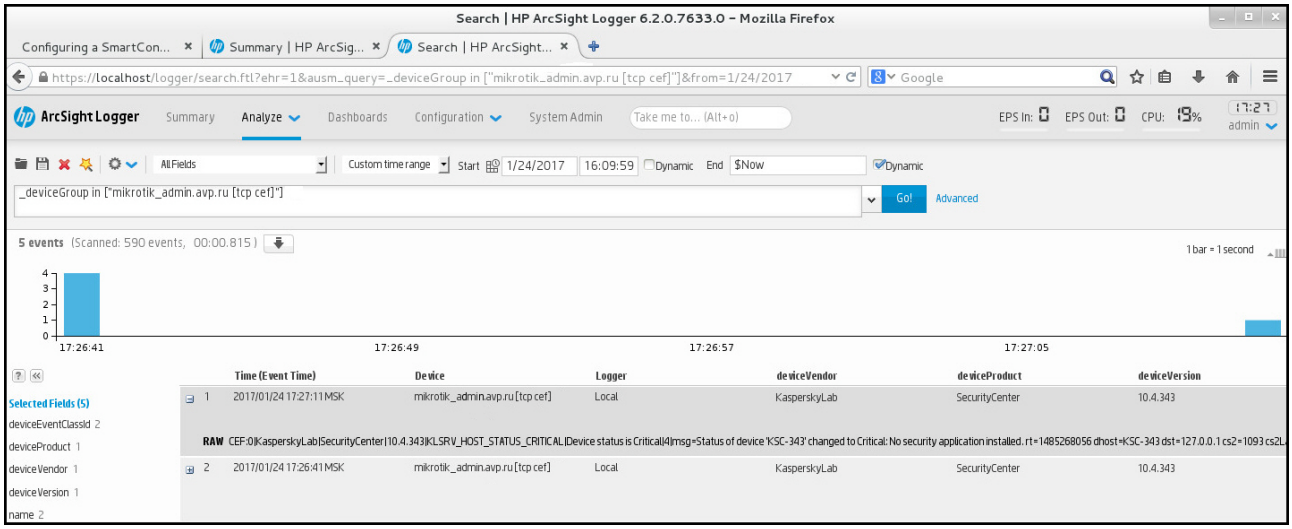



Figure 11. Пример событий

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

# Использование SNMP для отправки статистики программам сторонних производителей

В этом разделе описывается, как получить информацию от Сервера администрирования с помощью SNMP-протокола в Windows. Kaspersky Security Center содержит SNMP-агент, который передает статистику работы Сервера администрирования программам сторонних производителей с помощью OID.

В этом разделе также содержится информация о действиях для решения проблем, которые могут возникнуть при использовании SNMP для Kaspersky Security Center.

## В этом разделе

kaspersky

## SNMP-агент и идентификаторы объектов

Для Kaspersky Security Center SNMP-агент реализован в виде динамической библиотеки `klsnmpag.dll`, которая регистрируется установщиком при установке Сервера администрирования. SNMP-агент работает внутри процесса `snmp.exe` (который является службой Windows). Программы сторонних производителей используют SNMP-протокол для получения статистики (которая представлена в виде счетчиков) производительности Сервера администрирования.

Каждый счетчик имеет уникальный *идентификатор объекта* (далее также OID, object identifier). Идентификатор объекта – это последовательность чисел, разделенных точками. Идентификаторы объектов Сервера администрирования начинаются с префикса 1.3.6.1.4.1.23668.1093. OID счетчика – это соединение этого префикса с суффиксом, описывающим счетчик. Например, счетчик со значением OID 1.3.6.1.4.1.23668.1093.1.1.4 имеет суффикс со значением 1.1.4.

Вы можете использовать SNMP-клиент (например, Zabbix) для контроля состояния вашей системы. Чтобы получить информацию, вы можете найти значение OID и ввести это значение в свой SNMP-клиент. Затем ваш SNMP-клиент вернет вам другое значение, которое характеризует состояние вашей системы.

Список счетчиков и типы счетчиков находятся в файле `adminkit.mib` на Сервере администрирования. *MIB* расшифровывается как Management Information Base. Вы можете импортировать и анализировать файлы `.mib` с помощью программы MIB Viewer, которая предназначена для запроса и отображения значений счетчиков.

## Получение имени счетчика строк из идентификатора объекта

Чтобы использовать идентификатор объекта (OID) для передачи информации программам сторонних производителей, вам может потребоваться получить имя счетчика строк из этого OID.

► *Чтобы получить имя счетчика строк из OID:*

1. Откройте в текстовом редакторе файл `adminkit.mib`, расположенный на Сервере администрирования.
2. Найдите пространство имен, описывающее первое значение (слева направо).

   Например, для суффикса OID 1.1.4 это будет `"counters" (::= { kladminkit 1 })`.
3. Найдите пространство имен, описывающее второе значение.

   Например, для суффикса OID 1.1.4 это будет `counters 1`, что означает `deployment`.
4. Найдите пространство имен, описывающее третье значение.

   Например, для суффикса OID 1.1.4 это будет `deployment 4`, что означает `hostsWithAntivirus`.

Имя счетчика строк – это объединение этих значений, например, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, и это соответствует идентификатору OID со значением 1.3.6.1.4.1.23668.1093.1.1.4.

kaspersky

## Значения идентификаторов объектов для SNMP

В таблице ниже приведены значения и описания идентификатора объекта (далее также OID), которые используются для передачи информации о производительности Сервера администрирования программам сторонних производителей.

*Таблица 74. Значения и описания параметров идентификаторов объектов для SNMP*

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| deploymentStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.1.1 | Статус развертывания. Статус может принимать одно из следующих значений:<br>• **Информационное сообщение**. Лицензия больше не действует для N устройств.<br>• **Предупреждение**. одно из следующих:<br>M устройств с установленными программами "Лаборатории Касперского" на N устройствах в группах Сервера администрирования (N > M).<br>Срок действия лицензии L истекает на N устройствах через M дней.<br>Задача T по установке программ успешно завершена на N устройствах, для M устройств требуется перезагрузка.<br>• **Предельный**. Срок действия лицензии истек для N устройств.<br>• **ОК**. Ничего из вышеперечисленного. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| noAntivirusSoftware | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.1 | Причина deploymentStatus показывает, что в группах Сервера администрирования слишком много устройств, на которых не установлены управляемые программы.<br>Значение равно 1 в случае обнаружения нескольких устройств без управляемых программ и 0 в другом случае. |
| remoteInstallTaskFailed | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.2 | Причина deploymentStatus показывает, что на некоторых устройствах не удалось выполнить задачу удаленной установки. Количество этих устройств можно получить с помощью hostsRemoteInstallFailed. |
| licenceExpiring | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.3 | Причина deploymentStatus показывает, что есть несколько устройств, у которых истекает срок действия лицензии через семь дней. Количество этих устройств можно получить с помощью hostsLicenseExpiring. |
| licenceExpired | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.1.2.4 | Причина deploymentStatus показывает, что есть несколько устройств, у которых срок действия лицензии истек. Вы можете узнать количество этих устройств с помощью hostsLicenseExpired. |
| hostsInGroups | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.3 | Количество устройств в группах Сервера администрирования. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| hostsWithAntivirus | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.4 | Количество устройств в группах Сервера администрирования с установленными управляемыми программами. |
| hostsRemoteInstallFailed | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.5 | Количество устройств, на которых не удалось выполнить задачу удаленной установки. |
| licenceExpiringSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.6 | Идентификатор лицензионного ключа, срок действия которого скоро истечет (менее чем через 7 дней). |
| licenceExpiredSerial | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.1.7 | Идентификатор лицензионного ключа, срок действия которого истек. |
| licenceExpiringDays | Unsigned32 | .1.3.6.1.4.1.23668.1093.1.1.8 | Количество дней до истечения срока действия лицензии. |
| hostsLicenceExpiring | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.9 | Количество устройств с лицензией, срок действия которой скоро истекает (менее чем через 7 дней). |
| hostsLicenceExpired | Counter32 | .1.3.6.1.4.1.23668.1093.1.1.10 | Количество устройств, у которых истек срок действия лицензии. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| updatesStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.2.1 | Состояние антивирусных баз. Статус может принимать одно из следующих значений:<br>• **Информационное сообщение**. Сервер администрирования не обновлялся более одного дня, и с момента установки программы прошло менее одного дня.<br>• **Предупреждение**. Сервер администрирования не обновлялся более одного дня.<br>• **Предельный**. Сервер администрирования не обновлялся более двух дней.<br>• **ОК**. Ничего из вышеперечисленного. |
| serverNotUpdated | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.1 | Эта причина показывает, что Сервер администрирования не обновлялся в течение долгого времени. Время, которое считается долгим, указывается в updatesStatus. |
| notUpdatedHosts | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.2.2.2 | Эта причина показывает, что некоторые устройства не обновлялись в течение долгого времени (**Критическое** – 7 дней и более, **Предупреждение** – 3 дня). Вы можете узнать количество этих устройств с помощью hostsNotUpdated. |
| lastServerUpdateTime | OCTET STRING | .1.3.6.1.4.1.23668.1093.1.2.3 | Дата последнего обновления антивирусных баз на Сервере администрирования. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| hostsNotUpdated | Counter32 | .1.3.6.1.4.1.23668.1093.1.2.4 | Количество устройств, на которых антивирусные базы не обновлены. |
| protectionStatus | INTEGER { ok(0), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.3.1 | Статус постоянной защиты. одно из следующих:<br>• **Предупреждение**. одно из следующих:<br>На устройстве, входящем в группу Сервера администрирования, обнаружено нарушение безопасности.<br>Из-за ошибок шифрования некоторые устройства изменили состояние защиты.<br>Полная проверка давно не выполнялась.<br>• **Предельный**. На некоторых устройствах в группах Сервера администрирования не работает антивирусная защита.<br>• **ОК**. Ничего из вышеперечисленного. |
| antivirusNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.1 | Эта причина показывает, что программа безопасности не работает на некоторых устройствах. Вы можете узнать количество этих устройств с помощью hostsAntivirusNotRunning. |
| realtimeNotRunning | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.2 | Эта причина показывает, что на некоторых устройствах постоянная защита не работает. Вы можете узнать количество этих устройств с помощью hostsRealtimeNotRunning. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| notCuredFound | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.4 | Эта причина показывает, что есть некоторые устройства, содержащие не вылеченные объекты. Вы можете узнать количество этих устройств с помощью hostsNotCuredObject. |
| tooManyThreats | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.5 | Эта причина показывает, что на некоторых устройствах обнаружены угрозы. Вы можете узнать количество этих устройств с помощью hostsTooManyThreats. |
| virusOutbreak | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.3.2.6 | Эта причина показывает статус вирусной атаки.<br>Значение равно 1, если определенное количество вирусов было обнаружено в течение определенного времени, и 0 в других случаях. Количество вирусов и время указывается на Сервере администрирования с помощью параметра Вирусная атака. |
| hostsAntivirusNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.3 | Количество устройств, на которых не запущены программы безопасности. |
| hostsRealtimeNotRunning | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.4 | Количество устройств, на которых не запущена постоянная защита. |
| hostsRealtimeLevelChanged | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.5 | Количество устройств с недопустимым уровнем постоянной защиты. |
| hostsNotCuredObject | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.6 | Количество устройств с не вылеченными объектами. |
| hostsTooManyThreats | Counter32 | .1.3.6.1.4.1.23668.1093.1.3.7 | Количество устройств, которые содержат угрозы. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| fullscanStatus | INTEGER { ok(0), info(1), warning(2), critical(3) } | .1.3.6.1.4.1.23668.1093.1.4.1 | Статус полной проверки. одно из следующих:<br>• **Информационное сообщение**. С момента установки программы прошло менее 7 дней.<br>• **Предупреждение**. Полная проверка не производилась более 7 дней с момента установки программы.<br>• **Предельный**. Полная проверка не производилась более 14 дней с момента установки программы.<br>• **ОК**. Ничего из вышеперечисленного. |
| notScannedLately | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.4.2.1 | Эта причина показывает, что на некоторых устройствах не выполнялась проверка в течение определенного времени. Вы можете узнать количество этих устройств с помощью hostsNotScannedLately. Время указывается в fullScanStatus. |
| hostsNotScannedLately | Counter32 | .1.3.6.1.4.1.23668.1093.1.4.3 | Количество устройств, на которых не выполнялась проверка в течение определенного времени. Время указывается в fullScanStatus. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| logicalNetworkStatus | INTEGER { ok(0), warning(1), critical(2) } | .1.3.6.1.4.1.23668.1093.1.5.1 | Состояние логической сети Сервера администрирования. одно из следующих:<br>• **Предупреждение**. Если есть устройства со статусом Предупреждение, к которым нет доступа, или если есть устройства, которые не принадлежат ни к какой группе Сервера администрирования.<br>• **Предельный**. Если есть устройства, контроль над которыми потерян Сервером администрирования, или есть устройства со статусом Критический, к которым нет доступа.<br>• **ОК**. Ничего из вышеперечисленного. |
| notConnectedLongTime | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.1 | Эта причина показывает, что некоторые устройства в течение долгого времени не были подключены к Серверу администрирования (7 дней и более для устройства со статусом **Предупреждение** и 4 дня для устройства со статусом **Критический**). Вы можете узнать количество этих устройств с помощью hostsNotConnectedLongTime. |
| controlLost | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.5.2.2 | Эта причина показывает, что есть устройства, контроль над которыми потерян Сервером администрирования. Вы можете узнать количество этих устройств с помощью hostsControlLost. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| hostsFound | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.3 | Количество обнаруженных Сервером администрирования устройств, не входящих ни в одну группу Сервера администрирования. |
| groupsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.4 | Количество групп Сервера администрирования. |
| hostsNotConnectedLongTime | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.5 | Количество устройств, которые долгое время не подключались к Серверу администрирования. Время, которое считается долгим, указывается в notConnectedLongTime. |
| hostsControlLost | Counter32 | .1.3.6.1.4.1.23668.1093.1.5.6 | Количество устройств, которые не контролируются Сервером администрирования. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| `eventsStatus` | `INTEGER { ok(0), warning(1), critical(2) }` | .1.3.6.1.4.1.23668.1093.1.6.1 | Состояние подсистемы событий. одно из следующих:<br>• **Предупреждение**. одно из следующих:<br>Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows.<br>Есть устройства с проблемами, связанные со статусом.<br>• **Предельный**. одно из следующих:<br>Хотя бы на одном устройство произошло событие с уровнем важности "Критическое".<br>Хотя бы на одном устройстве произошло событие с уровнем важности "Отказ функционирования".<br>Есть событие неудачного завершения задачи хотя бы на одном устройстве.<br>Устройства групп Сервера администрирования давно не выполняли поиск обновлений Windows.<br>Есть устройства с проблемами, связанные со статусом.<br>• **ОК**. Ничего из вышеперечисленного. |

| Значение идентификатора объекта | Числовой тип данных | OID | Описание |
|---|---|---|---|
| criticalEventOccured | INTEGER { off(0), on(1) } | .1.3.6.1.4.1.23668.1093.1.6.2.1 | Причина eventsStatus показывает, что на Сервере администрирования произошли критические события. Вы можете получить количество этих событий с помощью criticalEventsCount.<br>Значение равно 1, если есть хотя бы одно критическое событие на любом устройстве, и 0 в другом случае. |
| criticalEventsCount | Counter32 | .1.3.6.1.4.1.23668.1093.1.6.3 | Количество критических событий на Сервере администрирования. |

## Устранение неисправностей

В этом разделе перечислены решения нескольких типичных проблем, с которыми вы можете столкнуться при использовании SNMP-службы.

**Программа стороннего производителя не может подключиться к SNMP-службе**

Убедитесь, что в параметрах операционной системы Windows установлена поддержка SNMP. По умолчанию поддержка SNMP отключена.

► *Чтобы разрешить поддержку SNMP в Windows 10:*

1. Перейдите в **Панель управления**.
2. Откройте меню **Установка и удаление программ**.
3. Нажмите на **Включение или отключение компонентов Windows**.
4. В списке компонентов Windows перейдите к функции SNMP и нажмите на кнопку **ОК**.
5. Перейдите в **Панель управления** → **Администрирование** → **Службы**.
6. Выберите SNMP-службу и запустите ее.
7. Проверьте, работает ли прослушивание, проверив его с помощью netstat для UPD-порта.

Поддержка SNMP разрешена в Windows 10.

**SNMP-служба работает, но программа стороннего производителя не может получить никаких значений**

Разрешите трассировку SNMP-агента и убедитесь, что создан непустой файл. Это означает, что SNMP-агент зарегистрирован правильно и работает. После этого разрешите подключения от SNMP-службы в параметрах службы. Если служба работает на том же устройстве, что и SNMP-агент, список IP-адресов должен содержать либо IP-адрес этого устройства, либо loopback 127.0.0.1.

В Windows должна работать SNMP-служба, которая взаимодействует с агентами. Вы можете указать пути к SNMP-агентам в реестре Windows с помощью regedit.

- Для Windows 10:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

- Для Windows Vista и Windows Server 2008:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Вы также можете разрешить трассировку SNMP-агента с помощью regedit.

- Для 32-разрядных систем:

  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug

- Для 64-разрядных систем:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug

  "TraceLevel"=dword:00000004

  "TraceDir"="C:\\"

**Значения не соответствуют статусам Консоли администрирования**

Для снижения нагрузки на Сервер администрирования реализовано кеширование значений для SNMP-агента. Задержка между актуализацией кеша и изменяемыми значениями на Сервере администрирования может вызвать несоответствие между значениями, возвращаемыми SNMP-агентом, и фактическими. При работе с программами сторонних производителей следует учитывать возможную задержку.

# Приложения

В этом разделе содержится справочная и дополнительная информация, касающаяся использования Kaspersky Security Center.

## В этом разделе

kaspersky

# Дополнительные возможности

В этом разделе рассматривается ряд дополнительных функций программы Kaspersky Security Center, предназначенных для расширения возможностей централизованного управления программами на устройствах.

## В этом разделе



## Автоматизация работы Kaspersky Security Center. Утилита klakaut

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center.

## Работа с внешними инструментами

Kaspersky Security Center позволяет сформировать список *внешних инструментов* (далее также *инструментов*) – программ, которые вызываются для клиентского устройства из Консоли администрирования при помощи группы контекстного меню **Внешние инструменты**. Для каждого инструмента из списка создается отдельная команда меню, с помощью которой Консоль администрирования запускает соответствующую инструменту программу.

Программа запускается на рабочем месте администратора. В качестве аргументов командной строки программа может принимать атрибуты удаленного клиентского устройства (NetBIOS-имя, DNS-имя, IP-адрес). Подключение к удаленному устройству может выполняться при помощи туннелированного соединения.

По умолчанию для каждого клиентского устройства список внешних инструментов содержит следующие служебные программы:

- **Удаленная диагностика** – утилита удаленной диагностики Kaspersky Security Center.
- **Удаленный рабочий стол** – стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу".
- **Управление компьютером** – стандартный компонент Microsoft Windows.

► *Чтобы добавить или удалить внешние инструменты, а также изменить их параметры,*

в контекстном меню клиентского устройства выберите пункт **Внешние инструменты → Настроить внешние инструменты**.

В результате откроется окно **Внешние инструменты**. В этом окне можно добавлять внешние инструменты или изменять их параметры с помощью кнопок **Добавить** и **Изменить**. Чтобы удалить внешние инструменты, нажмите на кнопку удаления со значком красного крестика ( ).

## Режим клонирования диска Агента администрирования

Клонирование жесткого диска "эталонного" устройства является распространенным способом установки программного обеспечения на новые устройства. Если Агент администрирования на жестком диске "эталонного" устройства во время клонирования работает в обычном режиме, возникает следующая проблема:

После развертывания на новых устройствах эталонного образа диска с Агентом администрирования эти устройства отображаются в Консоли администрирования одним значком. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со значком в Консоли администрирования.

Избежать проблемы с неверным отображением новых устройств в Консоли администрирования после клонирования помогает специальный *режим клонирования диска Агента администрирования*. Используйте этот режим, если вы разворачиваете программное обеспечение (с Агентом администрирования) на новых устройствах путем клонирования диска.

В режиме клонирования диска Агент администрирования работает, но не подключается к Серверу администрирования. При выходе из режима клонирования Агент администрирования удаляет внутренние данные, из-за наличия которых Сервер администрирования связывает несколько устройств с одним значком в Консоли администрирования. По завершении клонирования образа "эталонного" устройства, новые устройства отображаются в Консоли администрирования нормально (отдельными значками).

### Сценарий использования режима клонирования диска Агента администрирования

1. Администратор устанавливает Агент администрирования на "эталонном" устройстве.
2. Администратор проверяет подключение Агента администрирования к Серверу администрирования с помощью утилиты klnagchk (см. стр. 722).
3. Администратор включает режим клонирования диска Агента администрирования.
4. Администратор устанавливает на устройство программное обеспечение, патчи и выполняет любое количество перезагрузок устройства.
5. Администратор выполняет клонирование жесткого диска "эталонного" устройства на любое число устройств.
6. Для каждой клонированной копии должны быть выполнены следующие условия:
   a. имя устройства изменено;
   b. устройство перезагружено;
   c. режим клонирования диска выключен.

**Включение и выключение режима клонирования диска с помощью утилиты klmover**

► *Чтобы включить или выключить режим клонирования диска Агента администрирования:*

1. Запустите утилиту klmover на устройстве с установленным Агентом администрирования, который нужно клонировать.

   Утилита klmover находится в папке установки Агента администрирования.

2. Чтобы включить режим клонирования диска, в командной строке Windows введите команду `klmover -cloningmode 1`.

   Агент администрирования переключается в режим клонирования диска.

3. Чтобы запросить текущее состояние режима клонирования диска, в командной строке введите команду `klmover -cloningmode`.

   В результате в окне утилиты отобразится информация о том, включен или выключен режим клонирования диска.

4. Чтобы выключить режим клонирования диска, в командной строке утилиты введите команду `klmover -cloningmode 0`.

## См. также:

Развертывание захватом и копированием образа устройства .....182

Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы.....868

## Подготовка эталонного устройства с установленным Агентом администрирования для создания образа операционной системы

Вы можете создать образ операционной системы эталонного устройства с установленным Агентом администрирования, а затем развернуть образ на сетевых устройствах. В этом случае вы создаете образ операционной системы эталонного устройства, на котором Агент администрирования еще не запущен. Если вы запустите Агент администрирования на эталонном устройстве до создания образа операционной системы, идентификация Сервера администрирования устройств, развернутых из образа операционной системы эталонного устройства, будет проблематичной.

► *Чтобы подготовить эталонное устройство для создания образа операционной системы:*

1. Убедитесь, что операционная система Windows установлена на эталонном устройстве, также установите другое программное обеспечение, которое вам нужно на этом устройстве.
2. На эталонном устройстве в параметрах сетевых подключений Windows отключите эталонное устройство от сети, в которой установлен Kaspersky Security Center.
3. На эталонном устройстве запустите локальную установку Агента администрирования с помощью файла setup.exe.

   Запускается мастер установки Агента администрирования Kaspersky Security Center. Следуйте далее указаниям мастера.

4. На странице **Сервера администрирования** мастера укажите IP-адрес Сервера администрирования.

   Если вы не знаете точный адрес Сервера администрирования, введите localhost. Вы можете изменить IP-адрес позже, используя утилиту klmover (см. стр. 715) с ключом `-address`.

5. На странице **Запустить программу** в мастере отключите параметр **Запустить программу в процессе установки**.
6. После завершения установки Агента администрирования не перезагружайте устройство перед созданием образа операционной системы.

   Если вы перезагрузите устройство, вы должны будете повторить весь процесс подготовки эталонного устройства для создания образа операционной системы.
7. На эталонном устройстве в командной строке запустите утилиту sysprep (см. стр. 807) и выполните следующую команду: `sysprep.exe /generalize /oobe /shutdown`.

Эталонное устройство готово к созданию образа операционной системы (см. стр. 809).

## См. также:

Режим клонирования диска Агента администрирования ..... 867

Развертывание захватом и копированием образа устройства ..... 182

## Настройка параметров получения сообщений от компонента Мониторинг файловых операций

Управляемые программы, такие как Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент, отправляют сообщения от компонента Мониторинг файловых операций в Kaspersky Security Center. Kaspersky Security Center позволяет также следить за неизменностью критически важных областей систем (например, веб-серверы, банкоматы) и оперативно реагировать на нарушения целостности таких систем. Для этого реализована поддержка получения сообщений от компонента Мониторинг файловых операций. Компонент Мониторинг файловых операций позволяет следить не только за файловой системой устройства, но и за ветками реестра, состоянием сетевого экрана и состоянием подключенного оборудования.

Требуется выполнить настройку Kaspersky Security Center, чтобы получать сообщения от компонента Мониторинг файловых операций без использования программ Kaspersky Security для Windows Server или Kaspersky Security для виртуальных сред Легкий агент.

► *Чтобы настроить параметры получения сообщений от компонента Мониторинг файловых операций:*

1. Откройте системный реестр устройства, на котором установлен Сервер администрирования, например, локально с помощью команды regedit в меню **Пуск → Выполнить**.
2. Перейдите в раздел:
   - Для 32-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Для 64-разрядных систем:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Создайте ключи:
   - Создайте ключ KLSRV_EVP_FIM_PERIOD_SEC, чтобы указать интервал времени подсчета числа обработанных событий. Задайте следующие параметры:

     a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_SEC.

b. Укажите тип ключа DWORD.

c. Задайте диапазон значений промежутка времени от 43 200 до 172 800 секунд. По умолчанию промежуток проверки равен 86 400 секунд.

- Создайте ключ KLSRV_EVP_FIM_LIMIT для ограничения количества принимаемых событий за указанный промежуток времени. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_LIMIT.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений принимаемых событий от 2000 до 50 000. По умолчанию количество событий равно 20 000.

- Создайте ключ KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC для подсчета событий с точностью до определенного промежутка времени. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений от 120 до 600 секунд. Временной интервал, установленный по умолчанию, составляет 300 секунд.

- Создайте ключ KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC, чтобы после указанного значения времени программа выполняла проверку того, что число событий, обработанных за промежуток времени, становится меньше заданного ограничения. Проверка выполняется при достижении ограничения приема событий. Если условие выполняется, возобновляется сохранение событий в базу данных. Задайте следующие параметры:

  a. Укажите название ключа KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC.

  b. Укажите тип ключа DWORD.

  c. Задайте диапазон значений от 600 до 3600 секунд. Временной интервал, установленный по умолчанию, составляет 1800 секунд.

Если ключи не созданы, используются значения по умолчанию.

4. Перезапустите службу Сервера администрирования.

Ограничения получения событий от компонента Мониторинга файловых операций будут настроены. Результаты работы компоненты Контроля целостности системы вы можете посмотреть в отчетах **Топ 10 правил Мониторинга файловых операций / Контроля целостности системы, наиболее часто срабатывающие на устройствах** и **Топ 10 устройств с правилами Мониторинга файловых операций / Контроля целостности системы, срабатывающими чаще всего**.

## Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;

- сжимает базу данных (если необходимо).

Задача *Обслуживание Сервера администрирования* поддерживает MariaDB версии 10.3 и выше. Если используется MariaDB версии 10.2 или ниже, администраторам следует обслуживать базу данных самостоятельно.

► *Чтобы создать задачу* Обслуживание Сервера администрирования*:*

1. В дереве консоли выберите узел того Сервера администрирования, для которого нужно создать задачу *Обслуживание Сервера администрирования*.
2. Выберите папку **Задачи**.
3. В рабочей области папки **Задачи** нажмите на кнопку **Создать задачу**.

   Запустится мастер создания задачи.
4. В окне мастера **Выбор типа задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
5. Если во время обслуживания нужно сжимать базу данных Сервера администрирования, в окне мастера **Параметры** установите флажок **Сжать базу данных**.
6. Следуйте дальнейшим шагам мастера.

Созданная задача отображается в списке задач в рабочей области папки **Задачи**. Для одного Сервера администрирования может выполняться только одна задача *Обслуживание Сервера администрирования*. Если задача *Обслуживание Сервера администрирования* для Сервера уже создана, создание еще одной задачи обслуживания Сервера администрирования невозможно.

## Доступ к общедоступным DNS-серверам

Если доступ к серверам "Лаборатории Касперского" через системный DNS невозможен, Kaspersky Security Center может использовать публичные DNS-серверы в следующем порядке:

1. Google Public DNS (8.8.8.8);
2. Cloudflare DNS (1.1.1.1);
3. Alibaba Cloud DNS (223.6.6.6);
4. Quad9 DNS (9.9.9.9);
5. CleanBrowsing (185.228.168.168).

Запросы к DNS-серверам могут содержать доменные адреса и общедоступный IP-адрес Сервера администрирования, так как программа устанавливает TCP/UDP-соединение с DNS-сервером. Если Kaspersky Security Center использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса. Чтобы отключить использование общедоступного DNS, используйте утилиту klscflag и введите следующую команду с правами администратора:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -
t d -v 1
```

Чтобы включить общедоступный DNS, введите следующую команду с правами администратора:

```
klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -
```

t d -v 0

## Окно Способ уведомления пользователей

В окне **Способ уведомления пользователя** можно настроить параметры уведомления пользователя об установке сертификата на мобильное устройство.

- **Показать ссылку в мастере**. При выборе этого варианта ссылка на инсталляционный пакет будет отображена на последнем шаге работы мастера подключения нового устройства.
- **Отправить ссылку пользователю**. При выборе этого варианта вы можете настроить параметры оповещения пользователя о подключении устройства.

В блоке параметров **По электронной почте** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью сообщений электронной почты. Этот способ оповещения доступен, только если настроен SMTP-сервер (см. стр. 292).

В блоке параметров **С помощью SMS** вы можете настроить параметры уведомления пользователя об установке сертификата на его мобильное устройство с помощью SMS-сообщений. Этот способ оповещения доступен, только если настроено SMS-оповещение.

По ссылке **Изменить сообщение** в блоках параметров **По электронной почте** и **С помощью SMS** просмотрите и при необходимости отредактируйте текст уведомления.

### См. также:

Установка сертификата пользователю.....802

## Раздел Общие

В этом разделе можно настраивать общие параметры профиля для мобильных устройств Exchange ActiveSync:

- **Имя**

  Название профиля.

- **Разрешить неинициализируемые устройства**

  Если этот параметр включен, устройствам, которым доступны не все параметры политики Exchange ActiveSync, разрешено подключение к Серверу мобильных устройств. Используя соединение, вы можете управлять мобильными устройствами Exchange ActiveSync. Например, вы можете установить пароли, настроить отправку электронных писем или просмотреть информацию об устройствах, такую как идентификатор устройства или статус политики.

  Если этот параметр выключен, вы не сможете подключиться к Серверу мобильных устройств и управлять мобильными устройствами Exchange ActiveSync.

  По умолчанию параметр включен. Вы можете выключить этот параметр, если не собираетесь управлять мобильными устройствами Exchange ActiveSync и получать информацию о них.

- **Период обновления (ч)**

  Если этот параметр включен, программа обновляет информацию о политике Exchange ActiveSync с интервалом, указанным в поле ввода.

  Если этот параметр выключен, информация о политике Exchange ActiveSync не

обновляется.

По умолчанию этот параметр включен. Период обновления составляет один час.

### Окно Выборка устройств

Выберите выборку из списка **Выборка устройств**. В списке перечислены выборки, заданные по умолчанию, и выборки, созданные пользователем.

Вы можете просмотреть подробную информацию о выборках устройств в рабочей области папки **Выборки устройств**.

### Окно Определение названия создаваемого объекта

В окне укажите название создаваемого объекта. Имя не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

### Раздел Категории программ

В этом разделе можно настроить распространение информации о категориях программ на клиентские устройства.

**Полная передача данных (для Агентов администрирования версии Service Pack 2 и ниже)**

Если выбран этот вариант, при изменении категории программ на клиентские устройства передаются все данные категории. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и ниже.

Передача только измененных данных (для Агентов администрирования версии Service Pack 2 и выше)

Если выбран этот вариант, при изменении категории программ на клиентские устройства передаются не все данные категории, а только те данные, которые были изменены. Этот вариант передачи данных используется для Агентов администрирования версии Service Pack 2 и выше.

См. также:

Создание категорий программ для политики Kaspersky Endpoint Security для Windows.....558

# Приложение. Сертифицированное состояние программы: параметры и их значения

Этот раздел содержит перечень параметров программы, влияющих на безопасное состояние программы, и безопасные значения (диапазоны значений) параметров в сертифицированной конфигурации.

Изменение каких-либо из перечисленных параметров с их значений (диапазона значений) в сертифицированном конфигурации на другие значения выводит программу из безопасного состояния.

*Таблица 75. Параметры и их значения для программы в сертифицированном состоянии*

| Параметр | Краткое описание и диапазон значений | Значение параметра для программы в сертифицированном состоянии |
|---|---|---|
| Месторасположение папки общего доступа | При установке Kaspersky Security Center папка общего доступа, которая по умолчанию называется KLSHARE, находится не в папке установки Сервера администрирования. По умолчанию указана папка <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. | Не в папке, где установлен Сервер администрирования Kaspersky Security Center. |
| Политики | Для каждой управляемой программы создана политика. | |
| Пароль на деинсталляцию Агента администрирования | В политике Агента администрирования установлен пароль на удаление Агента администрирования.<br>Возможные значения:<br>• установлен;<br>• снят. | Установлен. |
| Защита паролем политики Kaspersky Endpoint Security для Windows.<br>Параметр программы Kaspersky Endpoint Security для Windows, если эта программа установлена. | Защита паролем позволяет установить ограничение на управление всеми или отдельными функциями и параметрами Kaspersky Endpoint Security для Windows, снижая вероятность несанкционированного или непреднамеренного внесения изменений в работу программы.<br>Возможные значения:<br>• установлена;<br>• снята. | Установлена. |

| Параметр | Краткое описание и диапазон значений | Значение параметра для программы в сертифицированном состоянии |
|---|---|---|
| Автоматическое обновление модулей Агентов администрирования | Обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений.<br>Возможные значения:<br>• включен;<br>• выключен. | Выключен. |
| Установка применимых обновлений со статусом одобрения *Не определено* | Патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.<br>Возможные значения:<br>• включен;<br>• выключен. | Выключен. |
| Запуск задачи **Загрузка обновлений в хранилище** | Задача **Загрузка обновлений в хранилище** выполняет загрузку обновлений баз и программных модулей, которые копируются с источника обновлений и размещаются в папке общего доступа.<br>Возможные значения:<br>• вручную;<br>• автоматически по расписанию. | Автоматически по расписанию.<br>Рекомендуемый интервал запуска задачи – один раз в час. |
| Запуск задачи **Установка обновлений** | Задача **Установка обновлений** выполняет установку ранее загруженных в хранилище обновлений на клиентские устройства.<br>Возможные значения:<br>• вручную;<br>• автоматически по расписанию. | Автоматически, по завершении задачи **Загрузка обновлений в хранилище**. |

| Параметр | Краткое описание и диапазон значений | Значение параметра для программы в сертифицированном состоянии |
|---|---|---|
| Передача данных службе KSN | Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.<br>Возможные значения передачи данных программы службе KSN:<br>• отключена;<br>• включена. | Отключена. |
| Источник обновлений задачи **Загрузка обновлений в хранилище** | Источник обновлений баз и модулей управляемых программ "Лаборатории Касперского".<br>Возможные значения:<br>• Серверы обновлений "Лаборатории Касперского";<br>• Главный Сервер администрирования;<br>• Локальная или сетевая папка. | • Главный Сервер администрирования;<br>• Локальная или сетевая папка.<br>Источник обновлений *Серверы обновлений "Лаборатории Касперского"* удален, чтобы программа не передавала информацию на серверы обновлений "Лаборатории Касперского". |
| Способ активации Сервера администрирования | Возможные значения:<br>• с помощью файла ключа;<br>• с помощью кода активации. | С помощью файла ключа. |

| Параметр | Краткое описание и диапазон значений | Значение параметра для программы в сертифицированном состоянии |
|---|---|---|
| Служба прокси-сервера активации "Лаборатории Касперского" | Служба прокси-сервера активации "Лаборатории Касперского" используется для обеспечения передачи запросов на активацию от управляемых программ к серверам активации "Лаборатории Касперского".<br>Возможные значения:<br>• отключена;<br>• включена. | Отключена |
| Доверенные каналы с использованием SSL-протокола | Протокол SSL позволяет идентифицировать стороны, взаимодействующие при подключении (взаимодействие между Сервером администрирования и устройствами), осуществлять шифрование передаваемых данных и обеспечивать их защиту от изменения при передаче.<br>Возможные значения:<br>• используется;<br>• не используется. | Используется. |
| Права пользователей | Права обеспечивают доступ администраторов, пользователей и групп пользователей к разным функциям программы. | Минимально необходимые права настроены: только уполномоченные роли имеют права изменять параметры защиты. |
| Условия для статуса *Критический* | Набор условий при котором устройство принимает статус *Критический*. | Выбрано условие **Найдено много вирусов**. Параметр **Более чем** равен значению 0. |
| Максимальное количество событий, хранящихся в базе данных Сервера администрирования | Максимальное количество событий, которое хранится в базе данных Сервера администрирования, необходимое для проведения аудита программы. | Рекомендуется установить значение не меньше 400 000 событий. |

| Параметр | Краткое описание и диапазон значений | Значение параметра для программы в сертифицированном состоянии |
|---|---|---|
| Срок хранения событий | Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита программы. | Рекомендуется установить значения:<br>• Для событий с уровнем важности *Критические* – не меньше 180 дней.<br>• Для событий с уровнем важности *Предупреждение* – не меньше 90 дней.<br>• Для событий с уровнем важности *Информационное сообщение* – не меньше 30 дней. |
| Срок хранения ревизий изменений объектов | Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита программы. | Рекомендуется установить значение не меньше 90 дней. |
| Права доступа к возможностям шифрования | Права доступа пользователей и ролей пользователей к возможностям шифрования данных. | Запрещено. |
| Объявления "Лаборатории Касперского" | Объявления "Лаборатории Касперского" предоставляют информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. | Отключены. |

## См. также

Настройка эталонных значений параметров программы .....878

# Настройка эталонных значений параметров программы

Этот раздел содержит инструкции по установке эталонных значений параметров программы. Настройка программы по эталонным параметрам необходима для работы сертифицированной конфигурации программы.

**Месторасположение папки общего доступа Сервера администрирования**

Папка должна находиться не в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа при установке Сервера администрирования:*

1. Запустите установку Сервера администрирования (см. стр. 217).

2. В окне **Папка общего доступа** мастера установки измените путь к папке общего доступа (см. стр. 250)

Расположение **Папки общего доступа Сервера администрирования** изменится на указанное.

► *Чтобы изменить папку общего доступа установленного Сервера администрирования:*

1. В дереве консоли выберите узел Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Папка общего доступа** измените расположение папки общего доступа.

Расположение **Папки общего доступа Сервера администрирования** изменится на указанное.

**Политики**

Для политики Агента администрирования необходимо установить пароль на удаление программы Агента администрирования. Для политики Kaspersky Endpoint Security для Windows необходимо настроить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows. В политике Kaspersky Endpoint Security для Windows необходимо настроить отправку уведомлений по электронной почте при возникновении событий об обнаружении вредоносного ПО.

**Пароль на деинсталляцию Агента администрирования**

Необходимо установить пароль на удаление программы Агента администрирования.

► *Чтобы установить пароль на деинсталляцию программы Агента администрирования:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Агент администрирования выберите пункт **Свойства**.
3. В окне свойств политики в разделе **Параметры** выберите установите флажок **Использовать пароль деинсталляции**.
4. Нажмите на кнопку **Изменить**.
5. В окне **Изменения пароля** введите пароль.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Пароль на удаление программы Агента администрирования установлен.

**Защита паролем политики Kaspersky Endpoint Security для Windows**

Необходимо установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows.

► *Чтобы установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows:*

1. В дереве консоли перейдите в папку **Политики**.
2. В контекстном меню политики Kaspersky Endpoint Security для Windows выберите пункт **Свойства**.
3. В окне свойств политики в разделе **Дополнительные параметры** выберите подраздел **Параметры программы**.

4. В разделе **Параметры программы** в блоке **Защита паролем** нажмите на кнопку **Настроить**.
5. В окне **Защита паролем** установите флажок **Включить защиту паролем**.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Защита паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows установлена.

**Автоматическое обновление модулей Агентов администрирования**

По умолчанию обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Необходимо отключить автоматическое обновление модулей Агента администрирования. Сертификации подлежат только определенные версии исполняемых модулей программы.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
3. В контекстном меню задачи выберите пункт **Свойства**.
4. В окне свойств задачи выберите раздел **Параметры**.
5. В подразделе **Прочие параметры** перейдите по ссылке **Настроить**.

   Откроется окно **Прочие параметры**.
6. Снимите флажок **Обновлять модули Агентов администрирования**.

   Если флажок снят, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
7. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей программы отключено.

Если в сети вашей организации назначены точки распространения, то для всех точек распространения также требуется отключить автоматическое обновление модулей Агента администрирования.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы точкой распространения:*

1. В дереве консоли выберите папку **Задачи**.
2. В папке **Задачи** выберите задачу **Загрузка обновлений в хранилище точек распространения**.
3. В контекстном меню задачи выберите пункт **Свойства**.
4. В окне свойств задачи выберите раздел **Параметры**.
5. В подразделе **Прочие параметры** перейдите по ссылке **Настроить**.

   Откроется окно **Прочие параметры**.
6. Снимите флажок **Обновлять модули Агентов администрирования**.

   Если флажок снят, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.

7. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей программы точкой распространения отключено.

**Установка применимых обновлений со статусом одобрения "Не определено"**

По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Необходимо отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

► *Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения* Не определено:

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агент администрирования.
3. В контекстном меню политики выберите пункт **Свойства**.
4. В разделе свойств политики **Управление патчами и обновлениями** снимите флажок **Устанавливать применимые обновления со статусом одобрения "Не определено"**.

   Если флажок **Устанавливать применимые обновления со статусом одобрения "Не определено"** снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.
5. Нажмите на кнопку **ОК**.

Автоматическая установка патчей "Лаборатории Касперского" со статусом одобрения *Не определено отключено.*

**Запуск задачи** Загрузка обновлений в хранилище Сервера администрирования **и** Загрузка обновлений в хранилища точек распространения

Необходимо настроить автоматический запуск задач **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**.

Рекомендуемый интервал автоматического запуска задач Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения** составляет один раз в час.

► *Чтобы настроить автоматический запуск задачи Сервера администрирования* ***Загрузка обновлений в хранилище Сервера администрирования*** *один раз в час:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Загрузка обновлений в хранилище Сервера администрирования** выберите пункт **Свойства**.
3. В окне свойств перейдите в раздел **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.
5. В поле **Интервал запуска (ч)** установите значение 1.
6. Нажмите на кнопку **ОК**.

   Автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** один раз в час настроен.

Если в сети организации назначены точки распространения, необходимо также настроить автоматический запуск задачи **Загрузка обновлений в хранилища точек распространения**. Для этого необходимо повторить действия, описанные выше для задачи **Загрузка обновлений в хранилище Сервера администрирования**.

**Запуск задачи** Установка обновлений

После выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** необходимо настроить запуск задачи **Установка обновлений**.

► *Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования**:*

1. В дереве консоли перейдите в папку **Задачи**.
2. В контекстном меню задачи **Установка обновлений** выберите пункт **Свойства**.
3. В окне свойств перейдите в раздел **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **По завершении другой задачи**.
5. В поле **Название задачи** выберите значение **Загрузка обновлений в хранилище Сервера администрирования**.
6. В поле **Результат выполнения** выберите значение **Завершена успешно**.
7. Нажмите на кнопку **ОК**.

Автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** настроен.

**Передача данных службе KSN**

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний (см. стр. 829).

Для работы программы в сертифицированной конфигурации службы, которые связаны с отправкой данных на внешние сервера и получением команд от внешних серверов (за периметром сети организации), должны быть отключены. Отключите передачу данных программой службе KSN.

► *Чтобы отключить передачу данных службе KSN:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно отключить передачу данных к службе KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
4. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".
5. При необходимости снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.
6. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

► *Чтобы отключить передачу данных службе KSN точкой распространения:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно отключить передачу данных к службе KSN.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Точки распространения**.
4. Выберите точку распространения и нажмите на кнопку Свойства.
5. В окне свойств точки распространения в разделе **Прокси-сервер KSN** выберите раздел **Параметры прокси-сервера KSN**.
6. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".
7. При необходимости снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.
8. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от точки распространения и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

Передача данных службе KSN должна быть отключена во всех управляемых программах.

Альтернативой отказу от использования KSN может стать использование Локального KSN (см. стр. 830). В этом случае вы получите доступ к оперативной базе знаний "Лаборатории Касперского", но информация о работе программ "Лаборатории Касперского" не будет передаваться на сервера "Лаборатории Касперского". Подробнее см. в разделе Kaspersky Security Network (KSN) (см. стр. 829).

**Источник обновлений задачи Загрузка обновлений в хранилище Сервера администрирования и задачи** Загрузка обновлений в хранилища точек распространения

Требуется отключить передачу данных программой службе обновлений "Лаборатории Касперского". Для отключения передачи данных программой серверу обновлений "Лаборатории Касперского" необходимо удалить серверы обновлений "Лаборатории Касперского" в задачах **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**.

► *Чтобы удалить серверы обновлений "Лаборатории Касперского" в задаче Загрузка обновлений в хранилище из источников обновлений:*

1. В дереве консоли перейдите в папку **Задачи**.

2. В контекстном меню задачи **Загрузка обновлений в хранилище Сервера администрирования** выберите пункт **Свойства**.
3. В окне свойств задачи перейдите в раздел **Параметры**.
4. В подразделе **Источники обновлений** перейдите по ссылке **Настроить**.
5. В окне **Источники обновлений** удалите значение *Серверы обновлений "Лаборатории Касперского"*.

Серверы обновления "Лаборатории Касперского" удалены из источника обновлений.

Настройку необходимо выполнить для задачи **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения** для всех точек распространения.

**Способ активации Сервера администрирования**

Сервер администрирования необходимо активировать только при помощи файлов ключа.

► *Чтобы активировать Сервер администрирования с помощью файла ключа:*

1. В дереве консоли выберите Сервер администрирования, который вы хотите активировать.
2. В контекстном меню Сервера администрирования выберите пункт **Все задачи** → **Мастер первоначальной настройки**.
3. В окне мастера **Выбор способа активации программы** нажмите на кнопку **Активировать программу с помощью файла ключа**.
4. В окне мастера **Активация программы** укажите файл ключа, на основании которого ключ будет добавлен в программу.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации программы с помощью кода активации программа регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа.

**Служба прокси-сервера активации "Лаборатории Касперского"**

Необходимо отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского":*

1. Откройте список служб вашего устройства.
2. Выберите в списке службу прокси-сервера активации "Лаборатории Касперского".
3. В контекстном меню службы выберите раздел **Свойства**.
4. В окне свойства службы на закладке **Общие** в поле **Тип запуска** выберите значение **Отключена**.
5. Нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

Служба прокси-сервера активации "Лаборатории Касперского" остановлена.

**Доверенные каналы с использованием SSL-протокола**

Для гарантированной доставки информации по доверенному каналу необходимо настроить использование SSL-соединений. В сертифицированной конфигурации программа должна использовать только доверенные

каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования:*

1. В дереве консоли перейдите в папку **Политики**.
2. В папке **Политики** выберите политику Агента администрирования.
3. В контекстном меню политики Агента администрирования выберите пункт **Свойства**.
4. В окне свойств Агента администрирования свойств в разделе **Сеть** выберите вложенный раздел **Сеть**.
5. Установите флажок **Использовать SSL-соединение**.
6. Нажмите на кнопку **ОК**.

   Если флажок установлен, подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.
7. В разделе **Подключения** выберите профиль подключения и нажмите на кнопку Свойства.
8. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.

   Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.
9. Нажмите на кнопку **ОК**.

Подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

**Права пользователей**

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в программе. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей:*

1. В дереве консоли выберите узел с именем необходимого Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования выберите раздел **Безопасность**.
4. В поле **Имена групп или пользователей** выберите пользователя или группу пользователей, которым нужно присвоить роль.

   Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.

   При добавлении пользователя по кнопке **Добавить** можно выбрать тип аутентификации пользователя (Microsoft Windows или Kaspersky Security Center). Аутентификация Kaspersky Security Center используется для выбора учетных записей внутренних пользователей, которые используются для работы с виртуальными Серверами администрирования.
5. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.
6. В окне **Роли пользователей** выберите роль для группы пользователей.

7. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

**Условия для статуса "Критический"**

При обнаружении на устройстве хотя бы одного вируса необходимо настроить на нем изменение статуса на *Критический*.

► *Чтобы настроить изменение статуса устройства на* Критический*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств перейдите в раздел **Статус устройства**.
3. В блоке **Условия для статуса Критический** установите флажок для условия **Найдено много вирусов**.
4. Для условия **Найдено много вирусов** установите значение *Более чем 0*.
5. Нажмите на кнопку **ОК**.

Изменение статуса устройства на *Критический*, при обнаружении на нем хотя бы одного вируса, настроено.

**Максимальное количество событий, хранящихся в базе данных Сервера администрирования**

Установите максимальное количество событий, хранящихся в базе данных Сервера администрирования, необходимое для проведения аудита программы. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить максимальное количество событий, хранящихся на Сервере.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Хранение событий**.
4. В поле **Максимальное количество событий, хранящихся в базе данных** установите рекомендуемое значение, не меньше 400 000 событий.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования, установлено.

По умолчанию емкость базы данных Сервера администрирования составляет 400 000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые.

**Срок хранения событий**

Для проведения аудита программы, необходимо настроить срок хранения событий в базе данных Сервера администрирования.

► *Чтобы изменить срок хранения событий:*

1. В дереве консоли выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Настройка событий**.
4. Установите время хранения событий по уровню их важности:
   - На закладке **Критическое событие** установите необходимое значение (не меньше 180 дней).
   - На закладке **Предупреждение** установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий изменен.

Срок хранения событий можно настроить также в свойствах политики Сервера администрирования.

► *Чтобы настроить срок хранения событий в свойствах политики Сервера администрирования:*

1. В дереве консоли выберите папку **Политики**.
2. В контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств политики Сервера администрирования перейдите в раздел **Настройка событий**.
4. Установите время хранения событий, в зависимости от уровня важности событий:
   - На закладке **Критическое событие** установите значение не меньше 180 дней.
   - На закладке **Предупреждение** установите значение не меньше 90 дней.
   - На закладке **Информационное сообщение** установите значение не меньше 30 дней.
5. Нажмите на кнопку **ОК**.

Срок хранения событий изменен.

**Срок хранения ревизии изменений объектов**

Необходимо настроить срок хранения ревизии объектов, необходимый для проведения аудита программы. Рекомендуемый срок хранения ревизии изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита программы.

► *Чтобы изменить срок хранения ревизии изменения объектов:*

1. В дереве консоли выберите Сервер администрирования, для которого необходимо настроить срок хранения изменений объектов.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Хранение истории ревизий**.

4. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.
5. Нажмите на кнопку **ОК**.

Срок хранения ревизии изменения объектов изменен.

**Права доступа к возможностям шифрования**

Настройте запрет доступа к возможностям шифрования данных для всех ролей и пользователей.

► *Чтобы запретить доступ роли к возможностям шифрованию данных:*

1. В дереве консоли выберите Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Роли пользователей**.
4. Выберите роль и нажмите на кнопку **Изменить**.
5. В окне свойств роли пользователей перейдите в раздел **Права**.
6. В блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранной запрещено.

► *Чтобы запретить доступ пользователя к возможностям шифрованию данных:*

1. В дереве консоли выберите Сервер администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Безопасность**.
4. Выберите пользователя и перейдите на закладку **Права**.
5. На закладке **Права** в блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранного пользователя запрещено.

**Контроль целостности исполняемых модулей программы**

Запустите утилиту klscmodchk для проверки целостности исполняемых модулей программы, как описано в инструкции (см. стр. 888).

**Выключение объявлений, связанных с безопасностью**

Выключите объявления "Лаборатории Касперского", связанные с безопасностью, как описано в инструкции (см. стр. 1458).

# Проверка целостности модулей с помощью утилиты klscmodchk

Программа Kaspersky Security Center содержит множество различных бинарных модулей в виде динамически подключаемых библиотек, исполняемых файлов, конфигурационных файлов и файлов интерфейса. Злоумышленники могут заменить один или несколько исполняемых модулей или файлов программы другими файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов программы, в программе Kaspersky Security Center предусмотрена проверка целостности компонентов программы с помощью утилиты klscmodchk. Утилита проверяет модули и файлы на наличие неавторизованных изменений

или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

**Включение проверки целостности модулей**

По умолчанию проверка целостности модулей при запуске программы выключена. Для включения проверки используются стандартные ключи реестра операционной системы Windows.

► *Чтобы включить проверку целостности модулей при запуске программы:*

1. Откройте реестр Windows устройства, на котором установлен Сервер администрирования, и добавьте новый ключ типа DWORD (32-разрядный) с именем `KLMODCHK_ENABLE_CHECKING` в соответствующую директорию:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags` для 32-разрядных систем;
   - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags` для 64-разрядных систем.
2. Используйте утилиту klscflag, чтобы установить ключ. Для этого в командной строке Windows введите следующую команду:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1.
   ```
3. Перезагрузите устройство с Сервером администрирования. При следующем запуске программы Kaspersky Security Center одновременно с Сервером администрирования запустится утилита klscmodchk, которая начнет проверку целостности модулей.

   Результаты всех автоматических проверок целостности (сообщения об успешной или неуспешной проверке, сообщения об ошибках), выполненных при запуске Сервера администрирования, записываются в журнал событий Kaspersky Event Log и доступны для просмотра в любой момент.

**Процедура проверки целостности модулей**

Проверка целостности модулей программы Kaspersky Security Center выполняется автоматически при каждом запуске программы, если эта опция была включена. Кроме того, проверку можно запустить в любое время вручную.

Утилита klscmodchk проверяет целостность модулей на основе файла манифеста kl_file_integrity_manifest.xml, который входит в состав сборки Kaspersky Security Center и расположен в папке установки программы. Файл манифеста содержит список проверяемых модулей программы, который формируется при ее установке.

Не рекомендуется вносить изменения в файл манифеста kl_file_integrity_manifest.xml, так как это приведет к изменению цифровой подписи файла и ошибкам в работе утилиты klscmodchk.

Чтобы проверить целостность файлов и модулей программы Kaspersky Security Center путем ручного запуска утилиты klscmodchk, выполните следующую команду в консоли командной строки:

```
integrity_checker [опции] [аргумент].
```

Для использования в команде доступны следующие опции:

- `--help` – выводит в консоль текст справки с описанием опций утилиты klscmodchk;

- `--version` – выводит в консоль номер версии утилиты klscmodchk;
- `--verbose` – выполняет расширенный вывод выполняемых действий и результатов (если эта опция не используется в команде, в консоли отображаются только ошибки, объекты, не прошедшие проверку, и суммарная статистика проверки);
- `--trace <имя файла>` – выполняет назначение файла для записи результатов проверки (если эта опция не используется в команде, результаты выводятся только в консоль), где `<имя файла>` — полный путь к файлу на диске.

В качестве аргумента командной строки используется значение `path_to_manifest`, после которого необходимо указать полный путь к файлу манифеста на диске.

# Особенности работы с интерфейсом управления

Этот раздел содержит описание приемов работы в главном окне Kaspersky Security Center.

## В этом разделе



## Дерево консоли

Дерево консоли (см. рис. ниже) предназначено для отображения сформированной в сети иерархии Серверов администрирования, структуры их групп администрирования, а также других объектов программы (например, папок **Хранилища** и **Управление программами**). Пространство имен Kaspersky Security Center может содержать несколько узлов с именами серверов, соответствующих установленным и включенным в структуру сети Серверам администрирования.

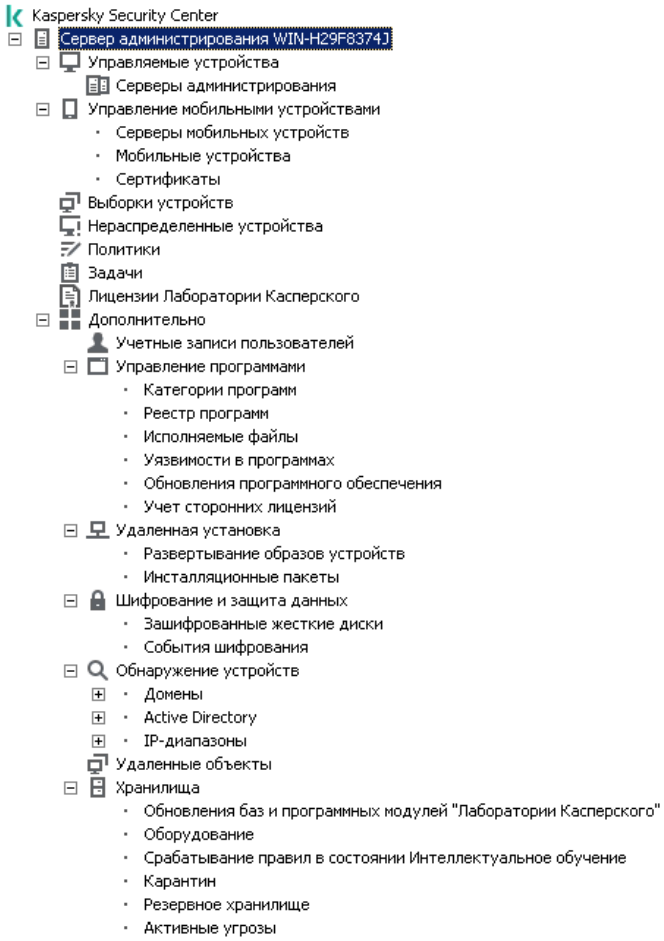



Figure 12. Дерево консоли

### Узел Сервер администрирования

Узел **Сервер администрирования – <Имя устройства>** является контейнером и отображает структурную организацию указанного Сервера администрирования.

В рабочей области узла **Сервер администрирования** содержится сводная информация о текущем состоянии программы и устройств, находящихся под управлением Сервера администрирования. Информация в рабочей области распределена по закладкам:

- **Мониторинг**. На закладке Мониторинг в реальном времени отображается информация о работе программы и текущем состоянии клиентских устройств. Важные сообщения для администратора (например, сообщения об уязвимостях, ошибках, обнаружении вирусов) выделяются цветом. По ссылкам на закладке **Мониторинг** можно выполнять типовые задачи администратора (например, установить и настроить программу безопасности на клиентских устройствах), а также переходить к другим папкам дерева консоли.
- **Статистика**. Содержит набор диаграмм, сгруппированных по темам (состояние защиты, антивирусная статистика, обновления и прочее). В диаграммах в визуальной форме представлена текущая информация о работе программы и состоянии клиентских устройств.
- **Отчеты**. Содержит шаблоны отчетов, формируемых программой. На закладке вы можете формировать отчеты из предустановленных шаблонов, а также создавать собственные шаблоны отчетов.

- **События**. Содержит записи о событиях, зарегистрированных во время работы программы. Для удобства чтения и сортировки записи распределены по тематическим выборкам. На закладке вы можете просмотреть выборки событий, сформированные автоматически, а также создать собственные выборки.

**Папки в составе узла Сервер администрирования**

В состав узла **Сервер администрирования – <Имя устройства>** входят следующие папки:

- **Управляемые устройства**. Папка предназначена для хранения, отображения, настройки и изменения структуры групп администрирования, групповых политик и групповых задач.
- **Управление мобильными устройствами**. Папка предназначена для управления мобильными устройствами. Папка **Управление мобильными устройствами** содержит следующие вложенные папки:
  - **Серверы мобильных устройств**. Предназначена для управления Серверами iOS MDM и Серверами мобильных устройства Exchange ActiveSync.
  - **Мобильные устройства**. Предназначена для управления мобильными устройствами KES, Exchange ActiveSync и iOS MDM.
  - **Сертификаты**. Предназначена для управления сертификатами мобильных устройств.
- **Выборки устройств**. Папка предназначена для быстрого выбора устройств, соответствующих определенным критериям (выборки устройств), среди всех управляемых устройств. Например, вы можете быстро выбрать устройства, на которых не установлена программа безопасности, и перейти к этим устройствам (просмотреть их список). С выбранными устройствами можно выполнять действия, например, назначать для них задачи. Вы можете использовать предустановленные выборки, а также создавать собственные (пользовательские) выборки.
- **Нераспределенные устройства**. В папке содержится список устройств, не входящих ни в одну группу администрирования. Вы можете выполнять действия с нераспределенными устройствами, например, перемещать их в группы администрирования, устанавливать на них программы.
- **Политики**. Папка предназначена для просмотра и создания политик.
- **Задачи**. Папка предназначена для просмотра и создания задач.
- **Лицензии "Лаборатории Касперского"**. Содержит список доступных лицензионных ключей для программ "Лаборатории Касперского". В рабочей области папки вы можете добавлять новые лицензионные ключи в хранилище лицензионных ключей, распространять лицензионные ключи на управляемые устройства, просматривать отчет об использовании лицензионных ключей.
- **Дополнительно**. Папка содержит набор вложенных папок, соответствующих различным группам функциональностей программы.

**Папка Дополнительно. Перемещение папок в дереве консоли**

В состав папки **Дополнительно** входят следующие папки:

- **Учетные записи пользователей**. Папка содержит список учетных записей пользователей сети.
- **Управление программами**. Папка предназначена для управления программами, установленными на устройствах в сети. Папка **Управление программами** содержит следующие вложенные папки:
  - **Категории программ**. Предназначена для работы с пользовательскими категориями программ.
  - **Реестр программ**. Содержит список программ на устройствах с установленным Агентом администрирования.

  - **Исполняемые файлы**. Содержит список исполняемых файлов, хранящихся на клиентских устройствах с установленным Агентом администрирования.
  - **Уязвимости в программах**. Содержит список уязвимостей в программах на устройствах с установленным Агентом администрирования.
  - **Обновления программного обеспечения**. Содержит список обновлений программ, полученных Сервером администрирования, которые могут быть распространены на устройства.
  - **Учет сторонних лицензий**. Содержит список групп лицензионных программ. С помощью групп лицензионных программ можно отслеживать использование лицензий на сторонние программы (не программы "Лаборатории Касперского") и нарушение лицензионных ограничений.
- **Удаленная установка**. Папка предназначена для управления удаленной установкой операционных систем и программ. Папка **Удаленная установка** содержит следующие вложенные папки:
  - **Развертывание образов устройств**. Предназначена для развертывания образов операционных систем на устройствах.
  - **Инсталляционные пакеты**. Содержит список инсталляционных пакетов, которые могут использоваться для удаленной установки программ на устройства.
- **Шифрование и защита данных**. Папка предназначена для управления процессом шифрования данных на жестких и съемных дисках.
- **Опрос сети**. Папка предназначена для отображения сети, в которой установлен Сервер администрирования. Информацию о структуре сети и входящих в ее состав устройствах Сервер администрирования получает в ходе регулярных опросов сети Windows, IP-диапазонов и Active Directory®, сформированных в сети организации. Результаты опросов отображаются в рабочих областях соответствующих папок: **Домены**, **IP-диапазоны** и **Active Directory**.
- **Хранилища**. Папка предназначена для работы с объектами, которые используются для мониторинга состояния устройств и их обслуживания. Папка **Хранилища** содержит следующие вложенные папки:
  - **Срабатывание правил в состоянии Интеллектуальное обучение**. Содержит список обнаружений, выполняемых правилами Kaspersky Endpoint Security, работающими в режиме Интеллектуального обучения на клиентских устройствах.
  - **Обновления и патчи ПО "Лаборатории Касперского"**. Содержит список обновлений, полученных Сервером администрирования, которые могут быть распространены на устройства.
  - **Оборудование**. Содержит список оборудования, подключенного к сети организации.
  - **Карантин**. Содержит список объектов, помещенных антивирусными программами в карантинные папки на устройствах.
  - **Резервное хранилище**. Папка содержит список резервных копий файлов, удаленных или измененных в процессе лечения на устройствах.
  - **Активные угрозы**. Содержит список файлов, для которых антивирусные программы определили необходимость отложенного лечения.

Вы можете изменять набор папок, вложенных в папку **Дополнительно**. Вложенные папки, которые активно используются, можно перемещать из папки **Дополнительно** на уровень выше. Папки, которые используются в работе редко, можно помещать в папку **Дополнительно**.

► *Чтобы переместить из папки **Дополнительно** вложенную папку:*

1. В дереве консоли выберите вложенную папку, которую вы хотите переместить из папки **Дополнительно**.

2. В контекстном меню вложенной папки выберите пункт **Вид** → **Переместить из папки Дополнительно**.

> Вы также можете вынести вложенную папку из папки **Дополнительно** в рабочей области папки **Дополнительно**, по ссылке **Переместить из папки Дополнительно** в блоке с названием вложенной папки.

► *Чтобы переместить папку в папку **Дополнительно**:*

1. В дереве консоли выберите папку, которую нужно переместить в папку **Дополнительно**.
2. В контекстном меню папки выберите пункт **Вид** → **Переместить в папку Дополнительно**.

См. также:

Основной сценарий установки.....92

## Как обновить данные в рабочей области

> В Kaspersky Security Center данные рабочей области (такие как статусы устройств, статистика и отчеты) никогда не обновляются автоматически.

► *Чтобы обновить данные в рабочей области, выполните одно из следующих действий:*

- нажмите на клавишу **F5**;
- в контекстном меню объекта в дереве консоли выберите пункт **Обновить**;
- Нажмите на значок обновления (  ) в рабочей области.

## Как перемещаться по дереву консоли

Для перемещения по дереву консоли вы можете использовать следующие кнопки, расположенные в панели инструментов:

-  – переход на один шаг назад;
-  – переход на один шаг вперед;
-  – переход на один уровень вверх.

Можно также воспользоваться навигационной цепочкой, расположенной в правом верхнем углу рабочей области. Навигационная цепочка содержит полный путь к той папке дерева консоли, в которой вы находитесь в текущий момент. Все элементы цепочки, кроме последнего, являются ссылками на объекты дерева консоли.

## Как открыть окно свойств объекта в рабочей области

Свойства большинства объектов Консоли администрирования можно изменять в окне свойств объекта.

► *Чтобы открыть окно свойств объекта, расположенного в рабочей области, выполните одно из следующих действий:*

- в контекстном меню объекта выберите пункт **Свойства**;
- выберите объект и нажмите комбинацию клавиш **ALT**+**ENTER**.

### Как выбрать группу объектов в рабочей области

Вы можете выбрать группу объектов в рабочей области. Выбор группы объектов можно использовать, например, для создания набора устройств и последующего формирования задач для него.

► *Чтобы выбрать диапазон объектов:*

1. Выберите первый объект диапазона и нажмите на клавишу **SHIFT**.
2. Удерживая нажатой клавишу **SHIFT**, выберите последний объект диапазона.

Диапазон будет выбран.

► *Чтобы объединить отдельные объекты в группу:*

1. Выберите первый объект в составе группы и нажмите на клавишу **CTRL**.
2. Удерживая нажатой клавишу **CTRL**, выберите остальные объекты группы.

Объекты будут объединены в группу.

### Как изменить набор граф в рабочей области

Консоль администрирования позволяет изменять набор граф, отображаемых в рабочей области.

► *Чтобы изменить набор граф в рабочей области:*

1. Выберите объект дерева консоли, для которого вы хотите изменить набор граф.
2. В рабочей области папки откройте окно настройки набора граф по ссылке **Добавить или удалить графы**.
3. В окне **Добавление или удаление граф** сформируйте набор граф для отображения.

## Справочная информация

В этом разделе в таблицах представлена сводная информация о контекстном меню объектов Консоли администрирования, а также о статусах объектов дерева консоли и рабочей области.

### В этом разделе

## Команды контекстного меню

В этом разделе содержится перечень объектов Консоли администрирования и соответствующий им набор пунктов контекстного меню (см. таблицу ниже).

*Таблица 76. Элементы контекстного меню объектов Консоли администрирования*

| Объект | Пункт меню | Назначение пункта меню |
|---|---|---|
| Общие пункты контекстного меню | **Поиск** | Открыть окно поиска устройств. |
| | **Обновить** | Обновить отображение выбранного объекта. |
| | **Экспортировать список** | Экспортировать текущий список в файл. |
| | **Свойства** | Открыть окно свойств выбранного объекта. |
| | **Вид → Добавить или удалить графы** | Добавить или удалить графы в таблице объектов в рабочей области. |
| | **Вид → Крупные значки** | Отображать объекты в рабочей области в виде крупных значков. |
| | **Вид → Мелкие значки** | Отображать объекты в рабочей области в виде мелких значков. |
| | **Вид → Список** | Отображать объекты в рабочей области в виде списка. |
| | **Вид → Таблица** | Отображать объекты в рабочей области в виде таблицы. |
| | **Вид → Настройка интерфейса** | Настроить отображение элементов Консоли администрирования. |
| **Kaspersky Security Center** | **Создать → Сервер администрирования** | Добавить в дерево консоли Сервер администрирования. |
| **<Имя Сервера администрирования>** | **Подключиться к Серверу администрирования** | Подключиться к Серверу администрирования. |
| | **Отключиться от Сервера администрирования** | Отключиться от Сервера администрирования. |
| **Управляемые устройства** | **Установить программу** | Запустить мастер удаленной установки программы. |
| | **Вид → Настройка интерфейса** | Настроить отображение элементов интерфейса. |
| | **Удалить** | Удалить Сервер администрирования из дерева консоли. |

| Объект | Пункт меню | Назначение пункта меню |
|---|---|---|
| | **Установить программу** | Запустить мастер удаленной установки для группы администрирования. |
| | **Обнулить счетчик вирусов** | Обнулить счетчики вирусов для устройств, входящих в состав группы администрирования. |
| | **Просмотреть отчет об угрозах** | Создать отчет об угрозах и вирусной активности устройств, входящих в состав группы администрирования. |
| | **Создать → Группу** | Создать группу администрирования. |
| | **Все задачи → Новая структура групп** | Создать структуру групп администрирования на основе структуры доменов или Active Directory. |
| | **Все задачи → Показать сообщение** | Запустить мастер создания сообщения для пользователей устройств, входящих в группу администрирования. |
| **Управляемые устройства → Серверы администрирования** | **Создать → Подчиненный Сервер администрирования** | Запустить мастер добавления подчиненного Сервера администрирования. |
| | **Создать → Виртуальный Сервер администрирования** | Запустить мастер создания виртуального Сервера администрирования. |
| **Управление мобильными устройствами → Мобильные устройства** | **Создать → Мобильное устройство** | Подключить новое мобильное устройство пользователя. |
| **Управление мобильными устройствами → Сертификаты** | **Создать → Сертификат** | Создать сертификат. |
| | **Создать → Мобильное устройство** | Подключить новое мобильное устройство пользователя. |
| **Выборки устройств** | **Создать → Новая выборка** | Создать выборку устройств. |
| | **Все задачи → Импортировать** | Импортировать выборку из файла. |
| **Лицензии "Лаборатории Касперского"** | **Добавить код активации или файл ключа** | Добавить лицензионный ключ в хранилище Сервера администрирования. |
| | **Активировать программу** | Запустить мастер создания задачи активации программы. |

| Объект | Пункт меню | Назначение пункта меню |
|---|---|---|
| | **Отчет об использовании лицензионных ключей** | Создать и просмотреть отчет о лицензионных ключах на клиентских устройствах. |
| **Управление программами → Категории программ** | **Создать → Категории** | Создать категорию программ. |
| **Управление программами → Реестр программ** | **Фильтр** | Настроить фильтр для списка программ. |
| | **Наблюдаемые программы** | Настроить публикацию событий об установке программ. |
| | **Удалить неустановленные программы** | Удалить из списка информацию о программах, которые уже не установлены на устройствах сети. |
| **Управление программами → Обновления программного обеспечения** | **Принять Лицензионные соглашения обновлений** | Принять Лицензионные соглашения обновлений программного обеспечения. |
| **Управление программами → Учет сторонних лицензий** | **Создать → Группу лицензионных программ** | Создать группу лицензионных программ. |
| **Удаленная установка → Инсталляционные пакеты** | **Показать актуальные версии программ** | Просмотреть список актуальных версий программ "Лаборатории Касперского", выложенных на интернет-серверах. |
| | **Создать → Инсталляционный пакет** | Создать инсталляционный пакет. |
| | **Все задачи → Обновить базы** | Обновить базы программ в инсталляционных пакетах. |
| | **Все задачи → Показать общий список автономных пакетов** | Просмотреть список автономных инсталляционных пакетов, созданных для инсталляционных пакетов. |

| Объект | Пункт меню | Назначение пункта меню |
|---|---|---|
| **Обнаружение устройств → Домены** | **Все задачи → Активность устройств** | Настроить параметры реакции Сервера администрирования на отсутствие активности устройств в сети. |
| **Обнаружение устройств → IP-диапазоны** | **Создать → IP-диапазон** | Создать IP-диапазон. |
| **Хранилища → Обновления баз и программных модулей "Лаборатории Касперского"** | **Загрузить обновления** | Открыть окно свойств задачи загрузки обновлений в хранилище Сервера администрирования. |
| | **Параметры загрузки обновлений** | Настроить параметры задачи загрузки обновлений в хранилище Сервера администрирования. |
| | **Отчет об используемых антивирусных базах** | Создать и просмотреть отчет о версиях баз. |
| | **Все задачи → Очистить хранилище обновлений** | Очистить хранилище обновлений на Сервере администрирования. |
| **Хранилища → Оборудование** | **Создать → Устройство** | Создать сетевое устройство. |

## Список управляемых устройств. Значение граф

В таблице ниже представлены названия и описания граф списка управляемых устройств.

*Таблица 77. Значение граф списка управляемых устройств*

| Название графы | Значение |
|---|---|
| Имя | NetBios-имя клиентского устройства. Описание значков имени устройств приведено в приложении (см. стр. 903). |
| Тип операционной системы | Тип операционной системы клиентского устройства. |
| Windows-домен | Наименование Windows-домена, в котором находится клиентское устройство. |
| Агент администрирования установлен | Результат установки на клиентское устройство Агента администрирования (*Да*, *Нет*, *Неизвестно*). |
| Агент администрирования запущен | Результат функционирования Агента администрирования (*Да*, *Нет*, *Нет данных*). |
| Постоянная защита | Установлена программа безопасности (*Да*, *Нет*, *Нет данных*). |
| Последнее подключение к Серверу администрирования | Время, прошедшее с момента соединения клиентского устройства с Сервером администрирования. |

| Название графы | Значение |
| --- | --- |
| Последнее обновление защиты | Время, прошедшее с момента последнего обновления управляемых устройств. |
| Статус | Текущий статус клиентского устройства (*ОК, Критический, Предупреждение)*. |
| Описание статуса | Причины изменения статуса клиентского устройства на *Критический* или *Предупреждение*.<br>Статус устройства изменяется на *Предупреждение* или *Критический* по следующим причинам:<br>• Программа безопасности не установлена.<br>• Обнаружено много вирусов.<br>• Уровень постоянной защиты отличается от уровня, установленного администратором.<br>• Давно не выполнялся поиск вредоносного ПО.<br>• Базы устарели.<br>• Давно не подключался.<br>• Обнаружены активные угрозы.<br>• Требуется перезагрузка.<br>• Установлены несовместимые программы.<br>• Обнаружены уязвимости в программах.<br>• Давно не выполнялась проверка обновлений Центра обновления Windows.<br>• Указанный статус шифрования.<br>• Параметры мобильного устройства не соответствуют политике.<br>• Есть необработанные инциденты.<br>• Статус устройства определен программой.<br>• На устройстве заканчивается дисковое пространство.<br>• Срок действия лицензии скоро истечет.<br>Статус устройства изменяется только на *Критический* по следующим причинам:<br>• Срок действия лицензии скоро истечет.<br>• Устройство стало неуправляемым.<br>• Защита выключена.<br>• Программа безопасности не запущена.<br>Управляемые программы "Лаборатории Касперского" на клиентских устройствах могут пополнять список описаний статусов. Kaspersky Security Center может получать описание статуса клиентского устройства от управляемых программ "Лаборатории Касперского" на этом устройстве. Если статус, присвоенный устройству управляемыми программами, не совпадает со статусом, присвоенным Kaspersky Security Center, в Консоли администрирования отображается статус, наиболее критичный для безопасности устройства. Например, если одна из управляемых программ присвоила устройству статус *Критический*, а Kaspersky Security Center – статус *Предупреждение*, то в Консоли администрирования для устройства отобразится статус *Критический* и описание этого статуса от управляемой программы. |

| Название графы | Значение |
|---|---|
| Последнее обновление информации | Время, прошедшее с момента последней успешной синхронизации клиентского устройства с Сервером администрирования (то есть с момента последнего опроса сети). |
| DNS-имя | Имя DNS-домена клиентского устройства. |
| DNS-домен | Основной DNS-суффикс. |
| IP-адрес | IP-адрес клиентского устройства. Рекомендовано использовать IPv4 адрес. |
| Последнее появление в сети | Продолжительность видимости клиентского устройства в сети. |
| Последняя полная проверка | Дата и время последней проверки клиентского устройства, выполненной программой безопасности по требованию пользователя. |
| Всего обнаружено угроз | Количество обнаруженных угроз. |
| Статус постоянной защиты | Статус постоянной защиты (*Запускается, Выполняется, Выполняется (максимальная защита), Выполняется (максимальная скорость), Выполняется (рекомендуемые параметры), Выполняется (с пользовательскими параметрами), Остановлена, Приостановлена, Сбой*). |
| IP-адрес соединения | IP-адрес подключения к Серверу администрирования Kaspersky Security Center. |
| Версия Агента администрирования | Версия Агента администрирования. |
| Версия программы | Версия программы безопасности, установленной на клиентском устройстве. |
| Последнее обновление антивирусных баз | Версия антивирусных баз. |
| Время начала последней сессии | Дата и время последнего включения клиентского устройства. |
| Требуется перезагрузка | Требуется перезагрузка клиентского устройства. |
| Точка распространения | Имя устройства, выполняющего роль точки распространения для этого клиентского устройства. |
| Описание | Описание клиентского устройства, полученное при сканировании сети. |
| Статус шифрования | Статус шифрования данных клиентского устройства. |

| Название графы | Значение |
|---|---|
| Состояние WUA | Состояние Агент Центра обновления Windows клиентского устройства.<br>Значение *Да* соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows от Сервера администрирования.<br>Значение *Нет* соответствует клиентским устройствам, которые получают обновления через Центр обновления Windows из других источников. |
| Архитектура операционной системы | Разрядность операционной системы клиентского устройства. |
| Статус защиты от спама | Статус компонента защиты от спама (*Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Нет данных от устройства*). |
| Статус защиты данных от утечек | Статус компонента защиты от утечки данных (*Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Нет данных от устройства*). |
| Статус защиты для серверов совместной работы | Статус компонента фильтрации содержимого (*Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Нет данных от устройства*). |
| Статус антивирусной защиты почтовых серверов | Статус компонента антивирусной защиты почтовых серверов (*Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Нет данных от устройства*). |
| Статус Endpoint Sensor | Статус компонента Endpoint Sensor (*Выполняется, Запускается, Остановлена, Приостановлена, Сбой, Нет данных от устройства*). |
| Создано | Время, когда значок <Имя устройства> был создан. Этот атрибут используется для сравнения различных событий друг с другом. |
| Имя виртуального или подчиненного Сервера. | Имя виртуального или подчиненного Сервера. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования. |
| Родительская группа | Название группы администрирования (см. стр. 81), в которой находится значок <Имя устройства>. Эта графа доступна только в списках, содержащих устройства с разных Серверов администрирования. |
| Под управлением другого Сервера администрирования | Параметр может принимать одно из следующих значений:<br>• True – если при удаленной установке программ безопасности на устройство окажется, что устройством управляет другой Сервер администрирования.<br>• False в противном случае. |

| Название графы | Значение |
|---|---|
| Номер сборки операционной системы | Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки (см.стр. 604), кроме указанного. |
| Номер выпуска операционной системы | Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска (см. стр. 604), кроме указанного. |

## Статусы устройств, задач и политик

В таблице ниже представлен список значков, отображающихся в дереве консоли и в рабочей области Консоли администрирования рядом с именами устройств, задач и политик. Эти значки характеризуют статус объектов.

*Таблица 78. Статусы устройств, задач и политик*

| Иконка | Состояние |
|---|---|
|  | Устройство с операционной системой для рабочих станций, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. |
|  | Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *ОК*. |
|  | Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Предупреждение*. |
|  | Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, со статусом *Критический*. |
|  | Устройство с операционной системой для рабочих станций, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно. |
|  | Устройство с операционной системой для серверов, обнаруженное в сети и не входящий в состав какой-либо группы администрирования. |
|  | Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *ОК*. |
|  | Устройство с операционной системой для серверов, входящее в состав группы администрирования, со статусом *Предупреждение*. |

| Иконка | Состояние |
|---|---|
|  | Устройство с операционной системой для серверов, входящий в состав группы администрирования, со статусом *Критический*. |
|  | Устройство с операционной системой для серверов, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно. |
|  | Мобильное устройство, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. |
|  | Мобильное устройство, входящее в состав группы администрирования, со статусом *ОК*. |
|  | Мобильное устройство, входящее в состав группы администрирования, со статусом *Предупреждение*. |
|  | Мобильное устройство, входящее в состав группы администрирования, со статусом *Критический*. |
|  | Мобильное устройство, входящее в состав группы администрирования, соединение которого с Сервером администрирования потеряно. |
|  | Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI в сети. |
|  | Устройство с защитой на уровне UEFI, обнаруженное в сети и не входящее в состав какой-либо группы администрирования. Устройство с защитой на уровне UEFI не в сети. |
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *ОК*. Устройство с защитой на уровне UEFI в сети. |
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *ОК*. Устройство с защитой на уровне UEFI не в сети. |
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI в сети. |
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Предупреждение*. Устройство с защитой на уровне UEFI не в сети. |

| Иконка | Состояние |
|---|---|
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI в сети. |
|  | Устройство с защитой на уровне UEFI, входящее в состав группы администрирования, со статусом *Критический*. Устройство с защитой на уровне UEFI не в сети. |
|  | Активная политика. |
|  | Неактивная политика. |
|  | Активная политика, унаследованная от группы, созданной на главном Сервере администрирования. |
|  | Активная политика, унаследованная от группы верхнего уровня иерархии. |
|  | Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Ожидает выполнения* или *Завершена успешно*. |
|  | Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Выполняется*. |
|  | Задача (групповая, Сервера администрирования или для наборов устройств) в состоянии *Сбой*. |
|  | Задача, унаследованная от группы, созданной на главном Сервере администрирования. |
|  | Задача, унаследованная от группы верхнего уровня иерархии. |

## Значки статусов файлов в Консоли администрирования

Для упрощения работы с файлами в Консоли администрирования Kaspersky Security Center рядом с именами файлов отображаются значки (см. таблицу ниже). Значки сигнализируют о статусах, присвоенных файлам управляемыми программами "Лаборатории Касперского" на клиентских устройствах. Значки отображаются в рабочей области папок **Карантин**, **Резервное хранилище** и **Активные угрозы**.

Статусы присваиваются объектам программой Kaspersky Endpoint Security, установленной на клиентском устройстве, на котором находится объект.

*Таблица 79. Соответствие значков статусам файлов*

| Иконка | Состояние |
|---|---|
|  | Файл со статусом *Заражен*. |
|  | Файл со статусом *Предупреждение* или *Возможно зараженный.* |

| Иконка | Состояние |
|---|---|
|  | Файл со статусом *Добавлено пользователем*. |
|  | Файл со статусом *Ложное срабатывание*. |
|  | Файл со статусом *Вылечен*. |
|  | Файл со статусом *Удален*. |
|  | Файл в папке **Карантин** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус. |
|  | Файл в папке **Резервное хранилище** со статусом *Не заражен*, *Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус. |
|  | Файл в папке **Активные угрозы** со статусом *Не заражен, Защищен паролем* или *Необходимо отправить в "Лабораторию Касперского"*. Если рядом со значком нет описания статуса, это означает, что управляемая программа "Лаборатории Касперского" на клиентском устройстве передала Kaspersky Security Center неизвестный статус. |

# Поиск и экспорт данных

В этом разделе содержится информация о способах поиска данных и об экспорте данных.

## В этом разделе

kaspersky

## Поиск устройств

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Результаты поиска можно сохранить в текстовом файле.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования и его подчиненных Серверов.

► *Чтобы искать клиентские устройства, входящие в группу администрирования:*

1. В дереве консоли выберите папку группы администрирования.
2. В контекстном меню папки группы администрирования выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать нераспределенные устройства:*

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

► *Чтобы искать устройства независимо от того, входят они в состав групп администрирования или нет:*

1. В дереве консоли выберите узел **Сервер администрирования**.
2. В контекстном меню узла выберите пункт **Поиск**.
3. На закладках окна **Поиск** укажите критерии, по которым нужно выполнить поиск устройств, и нажмите на кнопку **Найти**.

В результате устройства, соответствующие заданным критериям поиска, отобразятся в таблице в нижней части окна **Поиск**.

В окне **Поиск** вы можете также искать группы администрирования и подчиненные Серверы администрирования с помощью раскрывающегося списка в правом верхнем углу окна. Поиск групп администрирования и подчиненных Серверов администрирования недоступен при открытии окна **Поиск** из папки **Нераспределенные устройства**.

Для поиска устройств вы можете использовать в полях ввода окна **Поиск** регулярные выражения (см. стр. 919).

Полнотекстовый поиск в окне **Поиск** доступен:

- на закладке **Сеть** в поле **Описание**;
- на закладке **Оборудование** в полях **Устройство**, **Поставщик** и **Описание**.

## См. также:

Параметры поиска устройств .....908

## Параметры поиска устройств

Ниже представлены описания параметров поиска управляемых устройств (см. стр. 907). Результаты поиска отображаются в таблице в нижней части окна.

### Сеть

На закладке **Сеть** можно настроить критерии поиска устройств на основании их сетевых данных:

- **Имя устройства или IP-адрес**

  Имя устройства в сети Windows (NetBIOS-имя), IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Отображаются все устройства, входящие в указанный Windows-домен.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Описание** допустимо использовать следующие символы:

  - Внутри одного слова:
    - *****. Заменяет любую строку длиной 0 и более символов.

    **Пример**:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

    **Пример**:

    Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

  - Для связи нескольких слов:
    - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

**Пример**:

Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

- **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

**Пример**:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

**Пример**:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

**Пример**:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Только клиентские устройства, управляемые другими Серверами администрирования, будут включены в выборку.
  - **Нет**. Только клиентские устройства, управляемые этим же Сервером администрирования, будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

**Теги**

На закладке **Теги** можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

- **Применять, если есть хотя бы один из выбранных тегов**

  Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

  Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

  По умолчанию параметр выключен.

- **Тег должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ

*, который заменяет любую строку длиной 0 и более символов.

По умолчанию выбран этот вариант.

- **Тег должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

**Active Directory**

На закладке **Active Directory** можно указать, что устройства следует искать в подразделении (OU) или группе Active Directory. Также можно включить в выборку устройства из всех дочерних подразделений указанного подразделения Active Directory. Чтобы выбрать устройства, укажите следующие параметры:

- **Устройство находится в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию параметр выключен.

- **Устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

**Сетевая активность**

На закладке **Сетевая активность** можно указать критерии поиска устройств на основании их сетевой активности:

- **Это устройство является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут включены устройства, являющиеся точками распространения.
  - **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не**

**разрывать соединение с Сервером администрирования** снят.

- **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- **Устройство в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

**Программа**

На закладке **Программа** можно указать критерии поиска устройств на основании выбранной управляемой программы:

- **Имя программы**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Устройство под управлением Kaspersky Security Center**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Программа безопасности установлена**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

  - **Да**. Программа включает в выборку устройства, на которых установлена программа безопасности.
  - **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
  - **Значение не выбрано**. Критерий не применяется.

**Операционная система**

На закладке **Операционная система** можно настроить следующие критерии поиска устройств на основании установленной на них операционной системы:

- **Версия операционной системы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются

в результаты поиска.

- **Разрядность операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Идентификатор выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

**Статус устройства**

На закладке **Статус устройства** можно указать критерии поиска устройств по статусу устройства от управляемой программы:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический* или *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК, Критический* или *Предупреждение*.

- **Статус устройства определен программой**

Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

**Компоненты защиты**

На закладке **Компоненты защиты** можно настроить параметры поиска клиентских устройств по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

  По умолчанию параметр выключен.

- **Всего обнаружено угроз**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

**Реестр программ**

На закладке **Реестр программ** можно настроить параметры поиска устройств в зависимости от того, какие программы на них установлены:

- **Имя программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки флажка названия полей ввода **Название программы**, **Версия программы** и **Статус**

**программы** меняются на **Имя обновления**, **Версия обновления** и **Статус** соответственно.

По умолчанию параметр выключен.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

  В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

**Иерархия Серверов администрирования**

На закладке **Иерархия Серверов администрирования**, установите флажок **Включая данные с подчиненных Серверов до уровня**, если вы хотите, чтобы информация, хранящаяся на подчиненных Серверах администрирования, учитывалась при поиске устройств, а в поле ввода можно указать уровень вложенности подчиненного Сервера администрирования, с которого учитывается информация при поиске устройств. По умолчанию флажок снят.

**Виртуальные машины**

На закладке **Виртуальные машины** можно настроить параметры поиска устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- **Является виртуальной машиной**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Неважно**.
  - **Нет**. Искомые устройства не должны являться виртуальными машинами.
  - **Да**. Искомые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да** или **Неважно**.

- **Часть Virtual Desktop Infrastructure**

  В раскрывающемся списке можно выбрать следующие элементы:

  - **Неважно**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

**Оборудование**

На закладке **Оборудование** можно настроить поиск клиентских устройств по установленному на них оборудованию:

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

  Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Частота процессора (МГц)**

  Диапазон частот процессора. Устройства с процессорами, соответствующими диапазону частот в полях ввода (включительно), будут включены в состав выборки.

- **Виртуальных ядер процессора**

  Диапазон количества виртуальных ядер процессора. Устройства с процессорами, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ)**

  Диапазон значений объема жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ)**

  Диапазон значений объема оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону в полях ввода (включительно), будут включены в состав выборки.

**Уязвимости и обновления**

На закладке **Уязвимости и обновления** можно настроить параметры поиска устройств по источнику обновлений Центра обновления Windows:

- **WUA переключен на Сервер администрирования**

  В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

  - **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
  - **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые

получают обновления Центра обновления Windows из другого источника.

**Пользователи**

На закладке **Пользователи** можно настроить параметры поиска устройств по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  Если параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся указанным пользователем.

- **Пользователь, когда-либо выполнявший вход в систему**

  Если параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

**Проблемы, связанные со статусом управляемых программ**

На закладке **Проблемы, связанные со статусом управляемых программ** можно настроить поиск по описаниям статусов устройств от управляемой программы:

- **Описание статуса устройства**

  Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

**Статусы компонентов управляемых программ**

На закладке **Статусы компонентов управляемых программ** можно настроить поиск по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу защиты данных от утечек (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, Сбой).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

**Шифрование**

- **Шифрование**

  Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56*, *AES128*, *AES192* и *AES256*.

**Облачные сегменты**

На закладке **Облачные сегменты** можно настроить поиск по принадлежности к облачным сегментам:

- **Устройство находится в облачном сегменте**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать сегмент поиска.

  Если также включен параметр **Включать дочерние объекты**, то поиск ведется по всем вложенным объектам указанного сегмента.

  В результаты поиска включаются устройства только из выбранного сегмента.

- **Устройство обнаружено с помощью API.**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

  - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.
  - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.
  - **Google Cloud.** Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google.
  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но недоступно для поиска с помощью API.
  - **Не задано**. Условие не применяется.

**Компоненты программы**

Этот раздел содержит список компонентов тех программ, которые имеют соответствующие плагины управления, установленные в Консоли администрирования.

В разделе **Компоненты программы** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранной программе:

- **Статус**

Поиск устройств в соответствии со статусом компонента, отправленным управляемой программой на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства*, *Остановлено*, *Запускается*, *Приостановлено*, *Выполняется*, *Сбой* или *Не установлено*. Если выбранный компонент программы, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

Статусы, отправленные программами:

- *Запускается* – компонент в настоящее время находится в процессе инициализации.
- *Выполняется* – компонент включен и работает правильно.
- *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемой программе.
- *Сбой* – во время выполнения операции компонента произошла ошибка.

- *Остановлено* – компонент отключен и в данный момент не работает.
- *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки программы.

В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемой программой. Этот параметр показывает, что программы не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одной из программ, установленных на устройстве, или устройство выключено.

- **Версия**

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

### См. также:

Использование регулярных выражений в строке поиска ..... 919

Поиск устройств ..... 907

## Использование масок в строковых переменных

Для строковых переменных допустимо использование масок. Для создания масок вы можете использовать следующие регулярные выражения:

- Знак подстановки (*) – любая строка длиной 0 или более символов.
- Вопросительный знак (?) – один любой символ.
- [<интервал>] – Заменяет один символ из заданного диапазона или множества.

  Например: [0–9] – любая цифра. [abcdef] – один из символов a, b, c, d, e, f.

## Использование регулярных выражений в строке поиска

Для поиска отдельных слов и символов вы можете использовать в строке поиска следующие регулярные выражения:

- *. Заменяет последовательность любого количества символов. Например, для поиска слов "Сервер", "Серверный" или "Серверная" в строке поиска нужно ввести выражение `Сервер*`.
- ?. Заменяет любой один символ. Например, для поиска слов "Окно" или "Окна" в строке поиска нужно ввести выражение `Окн?`.

  > Текст в строке поиска не может начинаться с ?.

- [<интервал>]. Заменяет один символ из заданного диапазона или множества. Например, для поиска любой цифры в строке поиска нужно ввести выражение `[0-9]`. Для поиска одного из символов a, b, c, d, e, f в строке поиска нужно ввести выражение `[abcdef]`.

Для полнотекстового поиска вы можете использовать в строке поиска следующие регулярные выражения:

- Пробел. Результат: все устройства, описания которых содержат любое из перечисленных слов. Например, для поиска фразы, содержащей слово "Подчиненный" или "Виртуальный" (или оба этих слова), в строке поиска нужно ввести выражение `Подчиненный Виртуальный`.
- Знак "плюс" (+), AND или &&. При написании перед словом обозначает обязательное наличие слова в тексте. Например, для поиска фразы, содержащей и слово "Подчиненный", и слово "Виртуальный", в строке поиска можно ввести выражения: `+ Подчиненный + Виртуальный`, `Подчиненный AND Виртуальный`, `Подчиненный && Виртуальный`.
- OR или ||. При написании между словами обозначает наличие одного или другого слова в тексте. Например, для поиска фразы, содержащей или слово "Подчиненный", или слово "Виртуальный", в строке поиска можно ввести выражения: `Подчиненный OR Виртуальный`, `Подчиненный || Виртуальный`.
- Знак "минус" (-). При написании перед словом обозначает обязательное отсутствие слова в тексте. Например, для поиска фразы, в которой должно присутствовать слово "Подчиненный", и должно отсутствовать слово "Виртуальный", нужно ввести в строке поиска выражение `+Подчиненный-Виртуальный`.
- `"<фрагмент текста>"`. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте. Например, для поиска фразы, содержащей словосочетание "Подчиненный Сервер", нужно ввести в строке поиска выражение `"Подчиненный Сервер"`.

Полнотекстовый поиск доступен в следующих блоках фильтрации:

- в блоке фильтрации списка событий по графам **Событие** и **Описание**;
- в блоке фильтрации учетных записей пользователей по графе **Имя**;
- в блоке фильтрации реестра программ по графе **Название**, если в блоке **Показывать в списке** выбран критерий фильтрации **без группировки**.

### Экспорт списков из диалоговых окон

В диалоговых окнах программы вы можете экспортировать в текстовые файлы списки объектов.

Экспорт списка объектов возможен для тех разделов диалогового окна, которые содержат кнопку **Экспортировать в файл**.

## Параметры задач

В этом разделе перечислены параметры задач Kaspersky Security Center.

### В этом разделе

kaspersky

## Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

### Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.
  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
  - **Запрашивать у пользователя**

    На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

    По умолчанию выбран этот вариант.
  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.
  - **Принудительно перезагружать через (мин)**

    После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.
  - **Принудительно закрывать программы в заблокированных сеансах**

    Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и

изменения не сохранены, программа не позволяет перезагрузить устройство.

Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:
  - **Параметры Запуск по расписанию:**
    - **Каждый N час**

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

    - **Каждый N день**

      Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

      По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    - **Каждую N неделю**

      Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

    - **N минут**

      Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

      По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

    - **Ежедневно (не поддерживает переход на летнее время)**

      Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

      Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

      По умолчанию задача запускается каждый день в текущее системное время.

    - **Еженедельно**

      Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то

задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  - **Задать адреса устройств вручную или импортировать из списка**

    Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

    Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:
  - **Учетная запись по умолчанию**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль**

    Пароль учетной записи, от имени которой будет запускаться задача.

**Параметры, заданные после создания задачи**

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
  - **Распределить по подгруппам**
  - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Дополнительные параметры расписания:
  - **Включать устройства перед запуском задачи функцией Wake-on-LAN за (мин)**

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройство после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройство после выполнения задачи**

Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше (мин)**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
  - Блок **Сохранять информацию о результатах**:
    - **На Сервере администрирования в течение (сут)**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

- **Хранить в журнале событий ОС на устройстве**

События программы, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

По умолчанию параметр выключен.

- **Хранить в журнале событий ОС на Сервере**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранять все события**

Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события, связанные с ходом выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности
- Параметры области действия задачи

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **Выборка устройств**

Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**

## Параметры задачи Загрузить обновления в хранилище Сервера администрирования

### Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**
- **Прочие параметры**

  **Принудительно обновить подчиненные Серверы**

  Если флажок установлен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

  По умолчанию параметр выключен.

**Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

**Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

По умолчанию параметр выключен.

**Параметры, заданные после создания задачи**

Вы можете задать следующие параметры только после создания задачи.

- Раздел **Параметры**, блок **Состав обновлений**

  **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий (см. стр. 459).

  По умолчанию параметр выключен.

- Раздел **Проверка обновлений**

  **Выполнять проверку обновлений перед распространением**

  **Задача проверки обновлений**

Эта задача проверяет загруженные обновления перед тем как распространить их на все устройства, для которых Сервер администрирования выбран в качестве источника обновлений.

В этом поле можно указать задачу *Проверка обновлений*, которая была создана ранее. Также вы можете создать другую задачу *Проверка обновлений*.

## См. также:


Общие параметры задач.....921

Создание задачи для загрузки обновлений в хранилище Сервера администрирования.....461

Проверка полученных обновлений .....470

## Параметры задачи загрузки обновлений в хранилища точек распространения

### Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Источники обновлений**
- **Прочие параметры → Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

### Параметры, заданные после создания задачи

Вы можете указать следующие параметры в разделе **Параметры**, в блоке **Состав обновлений**, только после создания задачи.

**Загрузить файлы различий** Этот параметр включает функцию загрузки файлов различий (см. стр. 459).

По умолчанию параметр выключен.

### См. также:

Общие параметры задач.....921

Создание задачи загрузки обновлений в хранилища точек распространения .....465

## Параметры задачи поиска уязвимостей и требуемых обновлений

### Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних программ.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на клиентском устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. 750)).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в программах**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления только если параметр **Соединяться с сервером обновлений для актуализации данных** включен и параметр **Активный** включен в группе параметров **Режим поиска обновлений Windows Update**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска обновлений Windows Update** или если параметр **Соединяться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Активный**.
- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Выключен**, Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

## См. также:

Общие параметры задач.....921

Поиск уязвимостей в программах .....522

## Параметры задачи установки требуемых обновлений и закрытия уязвимостей

### Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- **Задайте правила установки обновлений**

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений (см. стр. 550).

- **Начинать установку в момент перезагрузки или выключения устройства**

  Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

  Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

  Если этот параметр выключен, необходимо установить пререквизиты вручную.

  По умолчанию параметр выключен.

- **Разрешать установку новой версии программы при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

  Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая**

  Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине

значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

**Параметры, заданные после создания задачи**

Вы можете задать параметры, перечисленные в разделах ниже, только после создания задачи. Полное описание параметров задачи, см. в разделе Общие параметры задач (см. стр. 921).

- **Общие**. В этом разделе отображается общая информация о задаче. Также можно указать, на какие устройства должна применяться задача *Установка требуемых обновлений и закрытие уязвимостей*:
  - **Распределить по подгруппам**
  - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Обновления для установки

  В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.
- Пробная установка обновлений:
  - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
  - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.
  - **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
  - **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите выполнить проверку обновлений на части устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

### См. также:



# Глобальный список подсетей

В этом разделе приведена информация и глобальном списке подсетей, которые вы можете использовать в правилах.

Чтобы сохранить информацию о подсетях вашей сети, вы можете настроить глобальный список подсетей для каждого Сервера администрирования. Этот список позволит сопоставить пары {IP-адрес, маска} и физические единицы, такие как офисы филиалов. Вы можете использовать подсети из этого списка в сетевых правилах и параметрах.

### В этом разделе



## Добавление подсети в глобальный список подсетей

Вы можете добавлять подсети и их описание в глобальный список подсетей.

► *Чтобы добавить подсеть в глобальный список подсетей:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** перейдите в раздел **Список глобальных подсетей**.
4. Нажмите на кнопку **Добавить**.

   Откроется окно **Новая подсеть**.
5. Заполните следующие поля:
   - **Общие параметры**

     IP-адрес подсети, которую вы добавляете.
   - **Маска подсети**

     Маска подсети, которую вы добавляете.
   - **Имя**

     Имя подсети. Имя подсети должно быть уникальным для всего глобального списка подсетей. Если вы указали имя подсети, которое уже существует в списке, то ей будет добавлен индекс, например: ~~1, ~~2.

- **Описание**

Описание может содержать дополнительную информацию, например, о филиале, которому принадлежит эта подсеть. Этот текст возникает везде, где отображается список подсетей, например, в списке правил ограничения трафика.

Это поле не обязательно для заполнения и может быть пустым.

6. Нажмите на кнопку **ОК**.

Подсеть появится в списке подсетей.

### Просмотр и изменение свойств подсети в глобальном списке подсетей

Вы можете просматривать и изменять свойства подсетей в глобальном списке подсетей.

► *Чтобы просмотреть или изменить свойства подсети в глобальном списке подсетей:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. В контекстном меню Сервера администрирования выберите пункт **Свойства**.
3. В открывшемся окне **Свойства** выберите раздел **Список глобальных подсетей**.
4. В списке выберите требуемую подсеть.
5. Нажмите на кнопку **Свойства**.

   Откроется окно **Новая подсеть**.
6. Если необходимо, измените параметры (см. стр. 934) подсети.
7. Нажмите на кнопку **ОК**.

Если вы сделали изменения, то они будут сохранены.

## Использование Агента администрирования для Windows, macOS и Linux: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования (см. стр. 750) и инсталляционного пакета (см. стр. 212) зависят от операционной системы. В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, macOS и Linux.

*Таблица 80. Сравнение функций Агента администрирования*

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| **Установка** | | | |
| Автоматическое создание инсталляционного пакета Агента администрирования, после установки Kaspersky Security Center (см. стр. 180) | ✓ | — | — |

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| Принудительная установка с помощью соответствующих параметров задачи удаленной установки программ Kaspersky Security Center (см. стр. 186) | ✓ | ✓ | ✓ |
| Установка программ с помощью рассылки пользователям устройств ссылок на автономные пакеты, сформированные Kaspersky Security Center(см. стр. 188) | ✓ | ✓ | ✓ |
| Установка путем клонирования образа жесткого диска с операционной системой и установленным Агентом администрирования, средствами, предоставляемыми Kaspersky Security Center для работы с образами дисков (см. стр. 182) | ✓ | — | — |
| Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами (см. стр. 182) | ✓ | ✓ | ✓ |
| Установка программ с помощью сторонних средств удаленной установки программ (см. стр. 181) | ✓ | ✓ | ✓ |
| Установка вручную с помощью запуска инсталляторов программ на устройствах (см. стр. 188) | ✓ | ✓ | ✓ |
| Установка Агента администрирования в неинтерактивном режиме (см. стр. 193) | ✓ | ✓ | ✓ |
| Установка Агента администрирования в неинтерактивном режиме (см. стр. 206) | ✓ | ✓ | ✓ |
| Подключение клиентского устройства к Серверу администрирования вручную (см. стр. 715) | ✓ | ✓ | ✓ |

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 476) | ✓ | — | — |
| Автоматическое распространение лицензионного ключа (см. стр. 395) | ✓ | ✓ | ✓ |
| Принудительная синхронизация (см. стр. 726). | ✓ | ✓ | ✓ |
| **Точка распространения** | | | |
| Использование точки распространения (см. стр. 167). | ✓ | ✓ | ✓ |
| Автоматическое назначение точек распределения (см. стр. 167) | ✓ | ✓<br>Без использования проверки подлинности на уровне сети (NLA). | ✓<br>Без использования проверки подлинности на уровне сети (NLA). |
| Офлайн-модель получения обновлений (см. стр. 474) | ✓ | ✓ | ✓ |
| Опросы сети (см. стр. 325) | ✓<br>• Опрос IP-диапазонов<br>• Опрос сети Windows<br>• Опрос Active Directory | — | ✓<br>Опрос IP-диапазонов |
| Запуск службы прокси-сервер KSN на стороне точки распространения (см. стр. 481) | ✓ | — | ✓ |

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства (см. стр. 465) | ✓ | — Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows. | ✓ |
| Принудительная установка программ | ✓ | С ограничением: нельзя выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS. | С ограничением: нельзя выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS. |
| Использовать в качестве push-сервера (см. стр. 668) | ✓ | — | ✓ |
| **Работа с программами сторонних производителей** | | | |
| Удаленная установка программ на устройства (см. стр. 189) | ✓ | — | — |
| Обновления программного обеспечения (см. стр. 488) | ✓ | — | — |
| Настройка обновлений операционной системы в политике Агента администрирования (см. стр. 513) | ✓ | — | — |
| Просмотр информации об уязвимостях в программах (см. стр. 520) | ✓ | — | — |
| Поиск уязвимостей в программах (см. стр. 522). | ✓ | — | — |

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| Инвентаризация программного обеспечения, установленного на устройствах (см. стр. 570) | ✓ | — | — |
| **Виртуальные машины** | | | |
| Установка Агента администрирования на виртуальные машины (см. стр. 201) | ✓ | ✓ | ✓ |
| Оптимизация параметров для VDI (см. стр. 202) | ✓ | ✓ | ✓ |
| Поддержка динамических виртуальных машин (см. стр. 202) | ✓ | ✓ | ✓ |
| **Другое** | | | |
| Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows (см. стр. 721) | ✓ | — | — |
| Мониторинг состояния антивирусной защиты (см. стр. 654) | ✓ | ✓ | ✓ |
| Управление перезагрузкой устройств (см. стр. 720). | ✓ | — | — |
| Поддержка отката файловой системы (см. стр. 204) | ✓ | ✓ | ✓ |
| Использование Агента администрирования в качестве шлюза соединений (см. стр. 667) | ✓ | ✓ | ✓ |
| Менеджер соединений (см. стр. 727) | ✓ | ✓ | ✓ |
| Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению) (см. стр. 310) | ✓ | ✓ | — |
| Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk (см. стр. 722) | ✓ | ✓ | ✓ |
| Удаленное подключение к рабочему столу клиентского устройства (см. стр. 717) | ✓ | ✓ С помощью системы виртуальных сетевых вычислений (VNC). | — |

| Функция Агента администрирования | Windows | macOS | Linux |
|---|---|---|---|
| Загрузка автономного инсталляционного пакета с помощью мастера переноса данных | ✓ | ✓ | ✓ |
| Опрос Zeroconf (см. стр. 333) | — | — | ✓ |

## См. также:

Развертывание Агента администрирования и программы безопасности .....178

kaspersky

# Kaspersky Security Center 14.2 Web Console

В этом разделе описаны действия, которые вы можете выполнять с помощью Kaspersky Security Center 14.2 Web Console.

## В этом разделе

# Аппаратные и программные требования

**Сервер Kaspersky Security Center 14.2 Web Console**

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2,5 ГГц.
- ОЗУ: 8 ГБ.
- Объем свободного места на диске: 40 ГБ.

Поддерживаются следующие операционные системы:

Microsoft Windows (только 64-разрядные версии):

- Windows Server 2012 Server Core;
- Windows Server 2012 Datacenter;
- Windows Server 2012 Essentials;
- Windows Server 2012 Foundation;
- Windows Server 2012 Standard;
- Windows Server 2012 R2 Server Core;
- Windows Server 2012 R2 Datacenter;
- Windows Server 2012 R2 Essentials;
- Windows Server 2012 R2 Foundation;
- Windows Server 2012 R2 Standard;
- Windows Server 2016 Datacenter (LTSB);
- Windows Server 2016 Standard (LTSB);
- Windows Server 2016 (вариант установки Server Core) (LTSB);
- Windows Server 2019 Standard;
- Windows Server 2019 Datacenter;
- Windows Server 2019 Core;
- Windows Server 2022 Standard;
- Windows Server 2022 Datacenter;
- Windows Server 2022 Core;
- Windows Storage Server 2012;
- Windows Storage Server 2012 R2;
- Windows Storage Server 2016;
- Windows Storage Server 2019;

Linux (только 64-разрядные версии):

- Debian GNU/Linux 9.x (Stretch);

- Debian GNU/Linux 10.x (Buster);
- Debian GNU/Linux 11.x (Bullseye);
- Ubuntu Server 18.04 LTS (Bionic Beaver);
- Ubuntu Server 20.04 LTS (Focal Fossa);
- Ubuntu Server 22.04 LTS (Jammy Jellyfish);
- CentOS 7.x;
- Red Hat Enterprise Linux Server 7.x;
- Red Hat Enterprise Linux Server 8.x;
- Red Hat Enterprise Linux Server 9.x;
- SUSE Linux Enterprise Server 12 (все пакеты обновлений);
- SUSE Linux Enterprise Server 15 (все пакеты обновлений).
- Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим);
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды и мандатный режим);
- Astra Linux Common Edition 2.12;
- ALT Server 9.2;
- ALT Server 10;
- Альт 8 СП Сервер (ЛКНВ.11100-01);
- Альт 8 СП Сервер (ЛКНВ.11100-02);
- Альт 8 СП Сервер (ЛКНВ.11100-03);
- Oracle Linux 7;
- Oracle Linux 8;
- Oracle Linux 9;
- РЕД ОС 7.3 Сервер;
- РЕД ОС 7.3 Сертифицированная редакция.

Виртуальная машина на основе Kernel поддерживается следующими операционными системами, рекомендованными для виртуальных сред Kaspersky Security Center:

- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
- ALT Server 10 64-разрядная;
- Astra Linux Special Edition (Орел, Воронеж, Смоленск) 1.7.2 (включая режим замкнутой программной среды и мандатный режим);
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная;
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
- РЕД ОС 7.3 Сервер 64-разрядная;
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

**Клиентские устройства**

Клиентскому устройству для работы с Kaspersky Security Center 14.2 Web Console требуется только браузер.

Требования к аппаратному и программному обеспечению устройства соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center 14.2 Web Console.

Браузеры:

- Mozilla Firefox Extended Support Release 91.8.0 или более поздняя версия (релиз 91.8.0 выпущен 5 апреля 2022);
- Google Chrome 100.0.4896.88 или более поздняя версия (официальная сборка);
- Microsoft Edge 100 или более поздняя версия;

# О Kaspersky Security Center 14.2 Web Console

Kaspersky Security Center Web Console (далее также Kaspersky Security Center 14.2 Web Console) представляет собой программу (веб-приложение), предназначенную для контроля состояния системы безопасности сетей организации, находящихся под защитой программ "Лаборатории Касперского".

С помощью программы вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы "Лаборатории Касперского" на устройства вашей сети и управлять установленными программами;
- управлять политиками, сформированными для устройств вашей сети;
- управлять учетными записями пользователей;
- управлять задачами программ, установленных на устройствах сети;
- просматривать отчеты о состоянии системы безопасности;
- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам.

Kaspersky Security Center 14.2 Web Console предоставляет веб-интерфейс, который обеспечивает ваше взаимодействие с Сервером администрирования с помощью браузера. Сервер администрирования – это программа, которая служит для управления программами "Лаборатории Касперского", установленными на устройства вашей сети. Сервер администрирования связывается с устройствами вашей сети через защищенные (SSL) каналы связи. Когда вы с помощью браузера подключаетесь к Kaspersky Security Center 14.2 Web Console, браузер устанавливает с Сервером Kaspersky Security Center 14.2 Web Console защищенное (HTTPS) соединение.

Kaspersky Security Center 14.2 Web Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center 14.2 Web Console с помощью браузера, в окне которого отображаются страницы веб-портала программы.
2. С помощью элементов управления веб-портала вы выбираете команду, которую хотите выполнить. Kaspersky Security Center 14.2 Web Console выполняет следующие действия:
    - Если вы выбрали команду, связанную с получением информации (например, просмотр списка устройств), Kaspersky Security Center 14.2 Web Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их браузеру в удобном для отображения виде.

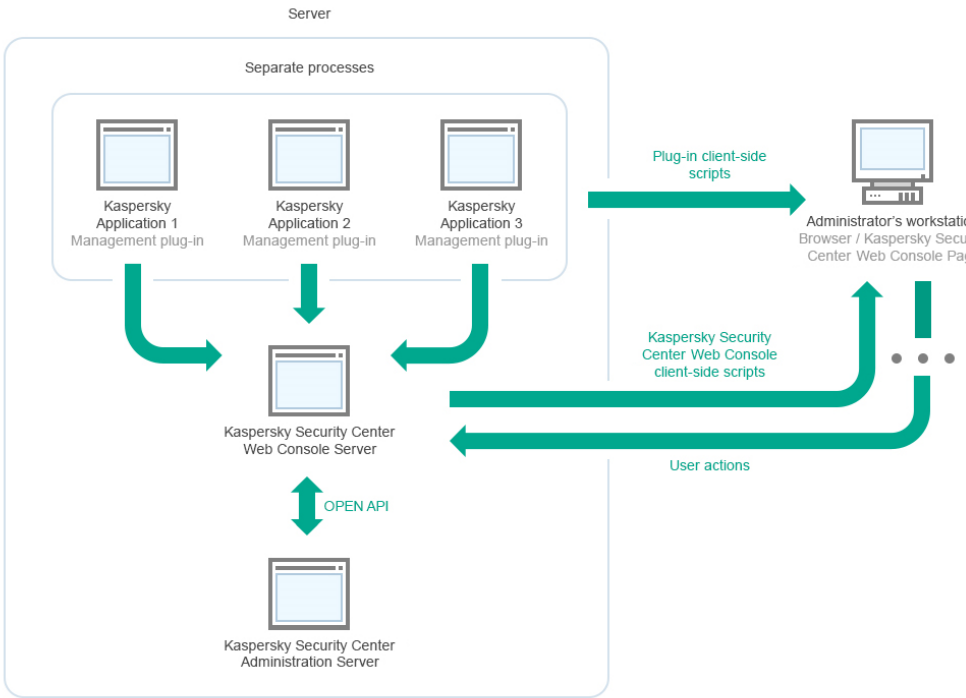
- Если вы выбрали команду управления (например, удаленная установка программы), Kaspersky Security Center 14.2 Web Console получает команду от браузера и передает ее Серверу администрирования. Затем программа получает результат выполнения команды от Сервера администрирования и передает результат браузеру в удобном для отображения виде.

Kaspersky Security Center 14.2 Web Console представляет собой многоязыковую программу. Вы можете изменить язык интерфейса в любое время без повторного открытия программы. Если вы устанавливаете Kaspersky Security Center 14.2 Web Console совместно с Kaspersky Security Center, Kaspersky Security Center 14.2 Web Console имеет тот же язык интерфейса что и установочный файл. Если вы устанавливаете только Kaspersky Security Center 14.2 Web Console, программа имеет тот же язык что и операционная система. Если Kaspersky Security Center 14.2 Web Console не поддерживает язык установочного файла или операционной системы, по умолчанию устанавливается английский язык.

Управление мобильными устройства не поддерживается в Kaspersky Security Center 14.2 Web Console. Однако если вы добавили мобильные устройства в группу администрирования в Консоли администрирования, эти устройства также отображаются в Kaspersky Security Center 14.2 Web Console.

# Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 14.2 Web Console

На следующем рисунке приведена схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 14.2 Web Console.




Развертывание плагинов управления программами "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждой программы), происходит одновременно с развертыванием сервера Kaspersky Security Center 14.2 Web Console.

Как администратор, вы имеете доступ к Kaspersky Security Center 14.2 Web Console через браузер на вашей рабочей станции.

Когда вы выполняете определенные действия в Kaspersky Security Center 14.2 Web Console, Kaspersky Security Center 14.2 Web Console взаимодействует с Сервером администрирования Kaspersky Security Center по OpenAPI. Kaspersky Security Center 14.2 Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center и отображает результаты ваших действий в Kaspersky Security Center 14.2 Web Console.

# Порты, используемые программой Kaspersky Security Center 14.2 Web Console

В таблице ниже перечислены порты, которые должны быть открыты на устройстве, на котором установлен Сервер Kaspersky Security Center 14.2 Web Console (далее также просто Kaspersky Security Center 14.2 Web Console).

*Таблица 81. Порты, используемые программой Kaspersky Security Center 14.2 Web Console*

| Номер порта | Имя службы | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 2001 | KSCWebConsolePlugin | HTTPS | API-порт, который используется процессами плагина управления для получения запросов от службы KSCWebConsoleManagementService. | Запуск процессов node.exe плагинов управления. |
| 1329, 2003 | KSCWebConsoleManagementService | HTTPS | API-порт, который используется для получения запросов от службы KSCWebConsole, работающей на том же устройстве. | Обновление компонентов Kaspersky Security Center 14.2 Web Console. |
| 2005 | KSCWebConsole | HTTPS | API-порт, который используется для получения запросов от службы KSCWebConsoleManagementService, работающей на том же устройстве. | Запуск установки Kaspersky Security Center 14.2 Web Console. |
| 3333 | Kaspersky OSMP KAS Service | HTTPS | Порт конечной точки авторизации OAuth2.0. | Identity and Access Management (IAM) |

| Номер порта | Имя службы | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 4004 | Kaspersky OSMP Facade Service | HTTPS | Порт провайдера идентификации OAuth2.0. | Identity and Access Management (IAM) |
| 4444 | Kaspersky OSMP KAS Service | HTTPS | Порт конечной точки самоанализа токена OAuth2.0 | Identity and Access Management (IAM) |
| 8200 | — | HTTP | API-порт, который используется для генерации сертификатов с помощью HashiCorp Vault (подробнее см. на сайте HashiCorp Vault https://www.vaultproject.io/). | Установка Kaspersky Security Center 14.2 Web Console и обновление компонентов Kaspersky Security Center 14.2 Web Console. |
| 4150, 4151, 4152 | KSCWebConsoleMessageQueue | HTTPS | API-порт Message Broker, который используется для связи между Kaspersky Security Center 14.2 Web Console и плагинами управления. | Взаимодействие между Kaspersky Security Center 14.2 Web Console и плагинов управления |

В таблице ниже перечислены порты, которые необязательно открывать на устройстве, на котором установлен Сервер Kaspersky Security Center 14.2 Web Console. Однако Kaspersky Security Center 14.2 Web Console использует эти порты для Identity and Access Manager (см. стр. 972).

*Таблица 82. Порты, используемые Kaspersky Security Center 14.2 Web Console для Identity and Access Manager*

| Номер порта | Имя службы | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 4445 | Kaspersky OSMP KAS Service | HTTPS | Основной порт Identity and Access Manager, который получает конфигурацию от Kaspersky Security Center 14.2 Web Console для порта конечной точки авторизации OAuth2.0 (подробнее о OAuth 2.0 см. веб-сайт OAuthhttps://www.oauth.com/ https://www.oauth.com) | Identity and Access Management (IAM) |

| Номер порта | Имя службы | Протокол | Назначение порта | Область |
|---|---|---|---|---|
| 2444 | Kaspersky OSMP Facade Service | HTTPS | Порт для настройки Identity and Access Manager | Identity and Access Management (IAM) |
| 2445 | Kaspersky OSMP Facade Service | HTTPS | Порт для подключения службы Kaspersky OSMP KAS Service к службе Kaspersky OSMP Facade Service | Identity and Access Management (IAM) |

См. также:

Порты, используемые Kaspersky Security Center ..... 98

Включение Identity and Access Manager: сценарий ..... 973

# Сценарий: Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console

В этом разделе описана установка Сервера администрирования Kaspersky Security Center 14 и Kaspersky Security Center 14.2 Web Console, первоначальная настройка Сервера администрирования с помощью мастера первоначальной настройки, а также установка программ "Лаборатории Касперского" на управляемые устройства с помощью мастера развертывания защиты.

Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console состоит из следующих этапов:

a. **Установка системы управления базами данных (СУБД)**

   Установите СУБД (см. стр. 164), используемую Kaspersky Security Center, или используйте существующую СУБД.

b. **Установка Сервера администрирования, Консоли администрирования и Агента администрирования**

   Вместе с Сервером администрирования устанавливаются также Консоль администрирования и серверная версия Агента администрирования.

   Во время установки Сервера администрирования Kaspersky Security Center (см. стр. 238) можно указать, требуется ли устанавливать на это же устройство Kaspersky Security Center 14.2 Web Console. Если вы решили установить оба компонента на одно устройство, то вам не потребуется устанавливать отдельно программу Kaspersky Security Center 14.2 Web Console, так как она будет установлена автоматически. Если вы хотите установить Kaspersky Security Center 14.2 Web Console на другое устройство, то после установки Сервера администрирования Kaspersky Security Center перейдите к установке Kaspersky Security Center 14.2 Web Console.

c. **Установка Kaspersky Security Center 14.2 Web Console**

   Если вы не выбрали на предыдущем шаге установку Kaspersky Security Center 14.2 Web Console совместно с Сервером администрирования Kaspersky Security Center, установите Kaspersky Security Center 14.2 Web Console на другом устройстве (см. стр. 950). Kaspersky Security Center 14.2 Web

Console можно установить отличном устройстве от устройства, на котором установлен Сервер администрирования.

**d. Выполнение первоначальной настройки**

После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается мастер первоначальной настройки (см. стр. 1007). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (см. стр. 1167) и задачи (см. стр. 1109) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. стр. 400).

**e. Лицензирование Kaspersky Security Center (если требуется)**

Kaspersky Security Center с поддержкой базовой функциональности (см. стр. 353) Консоли администрирования не требует лицензии. Вам необходима коммерческая лицензия, если вы хотите использовать одну или несколько дополнительных возможностей программы, включая Системное администрирование, Управление мобильными устройствами и интеграции с SIEM-системами. Вы можете добавить файл ключ или код активации для этих возможностей на соответствующем шаге (см. стр. 1013) мастера первоначальной настройки или вручную (см. стр. 1068).

**f. Обнаружение сетевых устройств**

Этот этап обрабатывается мастером первоначальной настройки (см. стр. 1007). Обнаружение устройств (см. стр. 324) можно также выполнить вручную. В результате Сервер администрирования Kaspersky Security Center получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center запускает обнаружение устройств регулярно, поэтому, если в сети появятся новые устройства, они будут обнаружены автоматически.

**g. Объединение устройств в группы администрирования**

Этот этап обрабатывается мастером первоначальной настройки (см. стр. 1007), но вы также можете переместить обнаруженные устройства в группы администрирования вручную.

**h. Установка Агента администрирования и программ безопасности на устройства в сети**

Развертывание защиты в сети организации подразумевает установку Агента администрирования и программ безопасности (например, Kaspersky Endpoint Security для Windows (см. стр. 1035)) на устройства, найденные Сервером администрирования в процессе обнаружения устройств.

Чтобы выполнить удаленную установку программы, запустите мастер развертывания защиты.

Программы безопасности защищают устройства от вирусов и других программ, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

Перед тем как установить Агент администрирования и программы безопасности на устройства в сети, убедитесь, что эти устройства доступны (включены).

**i. Распространение лицензионных ключей на клиентские устройства**

Распространите лицензионные ключи (см. стр. 389) на клиентские устройства, чтобы активировать управляемые программы безопасности на этих устройствах.

**j. Установка Kaspersky Security для мобильных устройств (если требуется)**

Если вы планируете управлять корпоративными мобильными устройствами, см. справку Kaspersky Security для мобильных устройств https://support.kaspersky.com/KESMob/10SP4MR3/ru-RU/218256.htm информацию о развертывании Kaspersky Endpoint Security для Android.

k. **Настройка политик программ "Лаборатории Касперского"**

Чтобы на различных устройствах были применены разные параметры программ, можно использовать управление безопасностью устройств или управление безопасностью, ориентированное на пользователей (см. стр. 404). Управление безопасностью устройств реализуется с помощью политик (см. стр. 1167) и задач (см. стр. 1109). Задачи могут выполняться только на устройствах, которые соответствуют определенным условиям. Для создания условий отбора устройств используются выборки устройств (см. стр. 1146) и теги (см. стр. 1159).

l. **Мониторинг состояния защиты сети**

Вы можете организовывать мониторинг сети с помощью веб-виджетов на информационной панели (см. стр. 1363), формировать отчеты (см. стр. 1368) о программах "Лаборатории Касперского", настраивать и просматривать выборки событий (см. стр. 1376), полученные от программ на управляемых устройствах, и просматривать список уведомлений.

# Установка

В этом разделе описана установка Kaspersky Security Center и Kaspersky Security Center 14.2 Web Console.

## В этом разделе



## Установка Kaspersky Security Center 14.2 Web Console

В этом разделе описано как установить Сервер Kaspersky Security Center 14.2 Web Console (далее также Kaspersky Security Center 14.2 Web Console) отдельно. Сначала необходимо установить систему управления базами данных (см. стр. 164) и Сервер администрирования Kaspersky Security Center (см. стр. 238). Вы можете установить Kaspersky Security Center 14.2 Web Console на том же устройстве, что и Kaspersky Security Center, или на другое.

► *Чтобы установить Kaspersky Security Center 14.2 Web Console:*

1. Запустите файл установки ksc-web-console-<номер_версии>.<номер сборки>.exe под учетной записью с правами администратора.

   Запускается мастер установки.
2. Выберите язык мастера установки.
3. В окне приветствия нажмите на кнопку **Далее**.
4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.

5. В окне **Папка назначения** выберите папку, в которую будет установлена программа Kaspersky Security Center 14.2 Web Console (по умолчанию %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Если такой папки нет, она будет создана автоматически в процессе установки.

   Вы можете изменить папку назначения с помощью кнопки **Обзор**.

6. В окне **Параметры подключения Kaspersky Security Center Web Console** укажите следующую информацию:

   - адрес Kaspersky Security Center 14.2 Web Console (по умолчанию 127.0.0.1);
   - порт, который Kaspersky Security Center 14.2 Web Console будет использовать для входящих подключений, то есть порт, который дает доступ к Kaspersky Security Center 14.2 Web Console из браузера (по умолчанию 8080).

   Рекомендуется оставить значения адреса и порта по умолчанию.

   Нажмите на кнопку **Проверить**, если хотите проверить, доступен ли выбранный порт.

   Если вы хотите включить запись в журнал Kaspersky Security Center 14.2 Web Console (см. стр. 1461), выберите соответствующий параметр. Если этот параметр не выбран, файлы журнала Kaspersky Security Center 14.2 Web Console не будут созданы.

7. В окне **Параметры учетной записи** укажите учетные записи и пароли.

   Рекомендуется использовать значения учетных записей по умолчанию.

8. В окне **Клиентский сертификат** выберите один из следующих вариантов:

   - **Сформировать новый**. Этот вариант рекомендуется использовать, если у вас нет сертификата браузера.
   - **Выбрать существующий**. Вы можете выбрать этот вариант, если у вас уже есть сертификат браузера. В этом случае укажите путь к сертификату.

   Если вы выбрали создать сертификат, при открытии Kaspersky Security Center 14.2 Web Console, браузер может информировать вас о том, что подключение к Kaspersky Security Center 14.2 Web Console не является приватным и что сертификат Kaspersky Security Center 14.2 Web Console недействителен. Это предупреждение появляется, так как сертификат Kaspersky Security Center 14.2 Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, вы можете выполнить одно из следующих действий:

   - Создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 112). Далее в окне **Выбрать существующий сертификат** включите параметр **Выбрать существующий сертификат** и укажите путь к пользовательскому сертификату.
   - Включите параметр **Создать новый сертификат** и добавьте сертификат Kaspersky Security Center 14.2 Web Console в список доверенных сертификатов браузера после установки Kaspersky Security Center 14.2 Web Console. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

   > Сертификаты в формате PFX не поддерживаются программой Kaspersky Security Center 14.2 Web Console. Чтобы использовать такой сертификат, необходимо сначала преобразовать его в поддерживаемый формат PEM (см. стр. 965) с помощью кроссплатформенной утилиты на основе OpenSSL, например, OpenSSL для Windows.

9. В окне **Доверенные Серверы администрирования** убедитесь, что ваш Сервер администрирования есть в списке, и нажмите на кнопку **Далее**, чтобы перейти к последнему окну мастера установки.

Если нужно добавить в список новый Сервер администрирования, нажмите на кнопку **Добавить**. В открывшемся окне укажите свойства нового доверенного Сервера администрирования:

- **Имя Сервера администрирования**

  Имя Сервера администрирования, которое будет отображаться в окне входа в Kaspersky Security Center 14.2 Web Console.

- **Адрес Сервера администрирования**

  IP-адрес устройства, на которое вы устанавливаете Сервер администрирования.

- **Порт Сервера администрирования**

  Порт OpenAPI, который Kaspersky Security Center 14.2 Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

- **Сертификат Сервера администрирования**

  Файл сертификата хранится на устройстве, на котором установлен Сервер администрирования. Путь к сертификату Сервера администрирования по умолчанию:

  - Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
  - Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.

  Если вы устанавливаете Kaspersky Security Center 14.2 Web Console на то же устройство, где установлен Сервер администрирования, используйте один из указанных выше путей. Или скопируйте файл сертификата с устройства, на котором установлен Сервер администрирования, на устройство, на котором вы устанавливаете Kaspersky Security Center 14.2 Web Console, и укажите локальный путь к сертификату.

10. В окне **Identity and Access Manager** укажите, хотите ли вы установить Identity and Access Manager (далее также IAM) (см. стр. 972). Если вы выбрали установку Identity and Access Manager, укажите следующие номера портов:

    - **KAS-порт администратора**. По умолчанию порт 4445 используется для получения конфигурации от Kaspersky Security Center 14.2 Web Console для порта конечной точки авторизации OAuth2.0.
    - **Фасадный порт администратора**. По умолчанию порт 2444 используется для настройки Identity and Access Manager.
    - **Фасадный порт взаимодействия**. По умолчанию порт 2445 используется для подключения Kaspersky OSMP KAS Service к Kaspersky OSMP Facade Service.

    Вы можете изменить номера портов по умолчанию. В дальнейшем вы не сможете изменить их с помощью Kaspersky Security Center 14.2 Web Console.

11. В последнем окне мастера установки нажмите на кнопку **Установить**, чтобы начать установку.

После успешного завершения установки на рабочем столе появляется ярлык и вы можете войти (см. стр. 970) в Kaspersky Security Center 14.2 Web Console.

Запускается мастер первоначальной настройки Сервера администрирования (см. стр. 1007), если он не был запущен в Консоли администрирования, интегрированной в Microsoft Management Console.

**Устранение неисправностей**

► *Если Kaspersky Security Center 14.2 Web Console не отображается в вашем браузере по указанному вами адресу, попробуйте сделать следующее:*

1. Проверьте правильность указанного имени или IP-адреса устройства, на котором установлена программа Kaspersky Security Center 14.2 Web Console.
2. Убедитесь, что устройство, на котором вы работаете, имеет доступ к устройству, на котором установлена программа Kaspersky Security Center 14.2 Web Console.
3. Убедитесь, что параметры сетевого экрана устройства, на котором установлена программа Kaspersky Security Center 14.2 Web Console, разрешают входящие подключения через порт 8080 и для приложения node.exe.
4. В Windows откройте окно **Службы**. Убедитесь, что запущена Kaspersky Security Center 14.2 Web Console.
5. Убедитесь, что у вас есть доступ к Kaspersky Security Center с помощью Консоли администрирования.
6. В Windows откройте окно **Просмотр событий** и выберите **Журнал приложений и служб** → **Kaspersky Event Log**. Убедитесь, что в журнале событий отсутствуют записи об ошибках.

### См. также:



# Особенности установки Kaspersky Security Center 14.2 Web Console на платформах Linux

В этом разделе описана процедура установки Сервер Kaspersky Security Center 14.2 Web Console (далее также Kaspersky Security Center 14.2 Web Console) на устройства с операционными системами Linux (см. список поддерживаемых дистрибутивов Linux (см. стр. 945)).

### В этом разделе



## Установка Kaspersky Security Center 14.2 Web Console на платформах Linux

В этом разделе описано, как установить Сервер Kaspersky Security Center 14.2 Web Console (далее также Kaspersky Security Center 14.2 Web Console) на устройства с операционными системами Linux. Сначала необходимо установить систему управления базами данных (см. стр. 164) и Сервер администрирования Kaspersky Security Center (см. стр. 238).

Используйте один из следующих установочных файлов, соответствующих дистрибутиву Linux, установленному на вашем устройстве:

- Для Debian: ksc-web-console-[номер_сборки].x86_64.deb.
- Для операционных систем на базе RPM: ksc-web-console-[номер_сборки].x86_64.rpm.
- Для Альт 8 СП: ksc-web-console-[номер_сборки]-alt8p.x86_64.rpm.

Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

► *Чтобы установить Kaspersky Security Center 14.2 Web Console:*

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center 14.2 Web Console, работает один из поддерживаемых дистрибутивов Linux (см. стр. 945).
2. Прочитайте Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center Linux не входит TXT файл с текстом Лицензионного соглашения, вы можете загрузить этот файл с сайта "Лаборатории Касперского"https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint. Если вы не согласны с условиями Лицензионного соглашения, не устанавливайте программу.
3. Создайте файл ответов (см. стр. 955), который содержит параметры для подключения Kaspersky Security Center 14.2 Web Console к Серверу администрирования. Имя файла ksc-web-console-setup.json. Файл расположен в следующей директории: /etc/ksc-web-console-setup.json.

   Пример файла ответов, содержащего минимальный набор параметров, адрес и порт по умолчанию:

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.c
   er|KSC Server",
     "acceptEula": true
   }
   ```

   При установке Kaspersky Security Center 14.2 Web Console на устройство с операционной системой ALT Linux необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

   Программа Kaspersky Security Center 14.2 Web Console не может быть обновлена с помощью того же установочного файла .rpm. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки программы, вы должны сначала удалить программу, а затем установить ее снова с новым файлом ответов.

4. Под учетной записью с привилегиями root используйте командную строку для запуска установочного файла с расширением .deb или .rpm, в зависимости от вашего дистрибутива Linux.
   - Чтобы установить или обновить предыдущую версию Kaspersky Security Center 14.2 Web Console из файла .deb, выполните следующую команду:

     ```
     $ sudo dpkg -i ksc-web-console-[номер_сборки].deb
     ```

   - Чтобы установить Kaspersky Security Center 14.2 Web Console из файла .rpm, выполните следующую команду:

     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[номер_сборки].x86_64.rpm
     ```

- Чтобы обновить предыдущую версию Kaspersky Security Center Web Console, выполните одну из следующих команд:
  - Для устройств с операционными системами RPM:

    ```
    $ sudo rpm -Uvh --nodeps --force ksc-web-console-[номер_сборки].x86_64.rpm
    ```

  - Для устройств с операционными системами Debian:

    ```
    $ sudo dpkg -i ksc-web-console-[номер_сборки].x86_64.deb
    ```

  Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки. Kaspersky Security Center 14.2 Web Console устанавливается в следующую директорию: /var/opt/kaspersky/ksc-web-console.

После завершения установки вы можете использовать браузер, чтобы открыть Kaspersky Security Center 14.2 Web Console и осуществить вход (см. стр. 970).

## Параметры установки Kaspersky Security Center 14.2 Web Console

Для установки Сервера Kaspersky Security Center 14.2 Web Console на устройства с операционными системами Linux (см. стр. 953)необходимо создать файл ответов (файл формата JSON), который содержит параметры подключения Kaspersky Security Center 14.2 Web Console к Серверу администрирования.

Пример файла ответов, содержащего минимальный набор параметров, адрес и порт по умолчанию:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
  "trusted":
"127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5".
}
```

При установке Kaspersky Security Center 14.2 Web Console на устройство с операционной системой ALT Linux необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

В таблице ниже описаны параметры, которые можно указать в файле ответов.

*Таблица 83. Параметры установки Kaspersky Security Center 14.2 Web Console на устройствах с операционными системами Linux*

| Параметр | Описание | Доступные значения |
|---|---|---|
| `address` | Адрес Сервера Kaspersky Security Center 14.2 Web Console (обязательный параметр). | Строковое значение. |
| `port` | Номер порта, который программа Kaspersky Security Center 14.2 Web Console использует для подключения к Серверу администрирования (обязательный параметр). | Числовое значение. |
| `defaultLangId` | Язык пользовательского интерфейса (по умолчанию `1033`). | Числовой код языка:<br>• Немецком: `1031`<br>• Английском: `1033`<br>• Испанском: `3082`<br>• Испанском (Мексика): `2058`<br>• Французском: `1036`<br>• Японском: `1041`<br>• Казахском: `1087`<br>• Польском: `1045`<br>• Португальском (Бразилия): `1046`<br>• Русском: `1049`<br>• Турецком: `1055`<br>• Китайском упрощенном: `4`<br>• Китайском традиционном: `31748`<br>Если значение не указано, используется английский язык. |
| `enableLog` | Включение или отключение журнала активности Kaspersky Security Center 14.2 Web Console (см. стр. 1461). | Логическое значение:<br>• `true` – включение журнала активности (выбрано по умолчанию).<br>• `false` – выключение журнала активности. |

| Параметр | Описание | Доступные значения |
| --- | --- | --- |
| `trusted` | Список доверенных Серверов администрирования, которым разрешено подключаться к Kaspersky Security Center 14.2 Web Console (обязательно). Для каждого Сервера администрирования должны быть заданы следующие параметры:<br>• адрес Сервера администрирования;<br>• порт OpenAPI, который используется программой Kaspersky Security Center 14.2 Web Console для подключения к Серверу администрирования (по умолчанию 13299);<br>• путь к сертификату Сервера администрирования;<br>• имя Сервера администрирования, которое будет отображаться в окне входа.<br>Параметры разделены символами вертикальной черты. Если указано несколько Серверов администрирования, разделите их двумя символами вертикальной черты. | Строковое значение следующего формата: `"server address\|port\|certificate path\|server name"`.<br>Пример: `"X.X.X.X\|13299\|/cert/server-1.cer\|Server 1\|\|Y.Y.Y.Y\|13299\|/cert/server-2.cer\|Server 2"`. |

| Параметр | Описание | Доступные значения |
|---|---|---|
| `acceptEula` | Принимаете ли вы условия Лицензионного соглашения (см. стр. 343). Файл, содержащий условия Лицензионного соглашения, загружается вместе с установочным файлом (обязательно). | Логическое значение:<br>• `true` – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. стр. 343).<br>• `false` – Я не принимаю условия Лицензионного соглашения (выбрано по умолчанию). |
| `certDomain` | Если вы хотите создать сертификат, используйте этот параметр, чтобы указать имя домена, для которого должен быть создан сертификат. | Строковое значение. |
| `certPath` | Если вы хотите использовать существующий сертификат, используйте этот параметр, чтобы указать путь к файлу сертификата. | Строковое значение.<br>Укажите путь `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"`, чтобы использовать существующий сертификат. Для пользовательского сертификата укажите путь к каталогу, в котором хранится этот сертификат. |
| `keyPath` | Если вы хотите использовать существующий сертификат, используйте этот параметр, чтобы указать путь к файлу ключа. | Строковое значение. |
| `webConsoleAccount` | Учетная запись, от имени которой работает служба KSCWebConsole. | Строковое значение следующего формата: `"group name:user name"`.<br>Пример: `"Group1:User1"`.<br>Если значение не указано, установщик Kaspersky Security Center 14.2 Web Console создает по умолчанию учетную запись `user_management_%uid%`. |

| Параметр | Описание | Доступные значения |
|---|---|---|
| managementServiceAccount | Учетная запись, от имени которой работает служба KSCWebConsoleManagement. | Строковое значение следующего формата: "group name:user name".<br>Пример: "Group1:User1".<br>Если значение не указано, установщик Kaspersky Security Center 14.2 Web Console создает по умолчанию учетную запись user_nodejs_%uid%. |
| serviceWebConsoleAccount | Учетная запись, от имени которой работает служба KSCSvcWebConsole. | Строковое значение следующего формата: "group name:user name".<br>Пример: "Group1:User1".<br>Если значение не указано, установщик Kaspersky Security Center 14.2 Web Console создает по умолчанию учетную запись user_svc_nodejs_%uid%. |
| pluginAccount | Учетная запись, от имени которой работает служба KSCWebConsolePlugin. | Строковое значение следующего формата: "group name:user name".<br>Пример: "Group1:User1".<br>Если значение не указано, установщик Kaspersky Security Center 14.2 Web Console создает по умолчанию учетную запись user_web_plugin_%uid%. |
| messageQueueAccount | Учетная запись, от имени которой работает служба KSCWebConsoleMessageQueue. | Строковое значение следующего формата: "group name:user name".<br>Пример: "Group1:User1".<br>Если значение не указано, установщик Kaspersky Security Center 14.2 Web Console создает по умолчанию учетную запись user_message_queue_%uid%. |

Если вы указываете параметры webConsoleAccount, managementServiceAccount, serviceWebConsoleAccount, pluginAccount или messageQueueAccount, убедитесь, что настраиваемые учетные записи пользователей принадлежат к одной и той же группе безопасности. Если эти параметры не указаны, установщик Kaspersky Security Center 14.2 Web Console создает группу безопасности по умолчанию, а затем создает в этой группе учетные записи пользователей с именами по умолчанию.

## См. также:

Порты, используемые Kaspersky Security Center.....98

kaspersky

# Установка Kaspersky Security Center 14.2 Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера "Лаборатории Касперского"

В этом разделе описывается установка Сервера Kaspersky Security Center 14.2 Web Console (далее также Kaspersky Security Center Web Console), который подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера "Лаборатории Касперского" или Microsoft. Перед установкой Kaspersky Security Center 14.2 Web Console установите систему управления базами данных (см. стр. 164) и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 257) или на узлы отказоустойчивого кластера Microsoft (см. стр. 260).

Если вы используете отказоустойчивый кластер Microsoft, не рекомендуется устанавливать Kaspersky Security Center 14.2 Web Console на узел отказоустойчивого кластера. В случае сбоя узла вы потеряете доступ к Серверу администрирования.

► *Чтобы установить Kaspersky Security Center 14.2 Web Console, которая подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера:*

1. Выполните шаги из раздела Установка Kaspersky Security Center 14.2 Web Console (см. стр. 950), начиная с шага 1 по шаг 8.
2. На шаге 9 в окне **Доверенные Серверы администрирования** нажмите на кнопку **Добавить**, чтобы добавить отказоустойчивый кластер в качестве доверенного Сервера администрирования.

   В открывшемся окне укажите следующие параметры:

   - **Имя Сервера администрирования**

     Имя кластера, которое будет отображаться в окне входа в Kaspersky Security Center 14.2 Web Console.

   - **Адрес Сервера администрирования.**

     В зависимости от типа отказоустойчивого кластера укажите адрес кластера:

     - **Отказоустойчивый кластер "Лаборатории Касперского"**. Укажите IP-адрес виртуального сетевого адаптера в качестве адреса кластера, если вы создали адаптер при подготовке узлов кластера (см. стр. 256). В противном случае укажите IP-адрес стороннего балансировщика нагрузки, который вы используете.
     - **Отказоустойчивый кластер Microsoft**. Укажите адрес кластера, который вы получили при создании отказоустойчивого кластера Microsoft.

   - **Порт Сервера администрирования.**

     Порт OpenAPI, который Kaspersky Security Center 14.2 Web Console, использует для подключения к Серверу администрирования (по умолчанию 13299).

   - **Сертификат Сервера администрирования**

     Сертификат Сервера администрирования находится в общем хранилище данных отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 255) или отказоустойчивого кластера Microsoft (см. стр. 262). Путь по умолчанию к файлу сертификата: <shared data folder>\1093\cert\klserver.cer. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center 14.2 Web Console. Укажите локальный путь к сертификату Сервера администрирования.

3. Продолжите стандартную установку (см. стр. 950) Kaspersky Security Center 14.2 Web Console.

После успешного завершения установки на рабочем столе появляется ярлык и вы можете войти (см. стр. 970) в Kaspersky Security Center 14.2 Web Console.

Если вы используете отказоустойчивый кластер "Лаборатории Касперского", вы можете перейти в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**, чтобы просмотреть информацию об узлах кластера и о файловом сервере (см. стр. 255).

## Обновление Kaspersky Security Center Web Console

Если вы хотите использовать новую версию Kaspersky Security Center Web Console, не удаляя установленный в данный момент экземпляр программы, вы можете использовать стандартную процедуру обновления, предусмотренную в установщике Kaspersky Security Center Web Console.

► *Чтобы обновить Kaspersky Security Center Web Console:*

1. Под учетной записью с правами администратора запустите ksc-web-console-<номер версии>.<номер сборки>.exe исполняемый файл, где <номер сборки> означает номер сборки Kaspersky Security Center Web Console, номер которой больше, чем у установленного вами экземпляра.
2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **ОК**.
3. В окне приветствия выберите параметр **Обновить** и нажмите на кнопку **Далее**.
4. В окне **Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения. Установка продолжится после принятия Лицензионного соглашения, в противном случае кнопка **Далее** недоступна.
5. Выполните все шаги мастера установки, пока не завершите установку. В процессе установки вы также можете изменить параметры Kaspersky Security Center Web Console, которые вы указали при предыдущей установке (см. стр. 950). Нажмите на кнопку **Обновить** на шаге **Все готово для изменения Kaspersky Security Center Web Console**. Дождитесь, пока новые параметры вступят в силу, и на следующем шаге мастера установки нажмите на кнопку **Готово**. Вы также можете перейти по ссылке **Запустить Kaspersky Security Center Web Console в вашем браузере** для немедленного запуска обновленного экземпляра Kaspersky Security Center Web Console.

   > Изменение параметров Kaspersky Security Center Web Console при обновлении доступно только в версии программы Kaspersky Security Center 12.2 Web Console и выше.

   Программа Kaspersky Security Center Web Console установлена.

### См. также

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Сценарий:Обновление Kaspersky Security Center и управляемых программ безопасности .....280

# Сертификаты для работы с Kaspersky Security Center 14.2 Web Console

В разделе описано, как выпустить и заменить сертификаты для Kaspersky Security Center 14.2 Web Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с Kaspersky Security Center 14.2 Web Console.

## См. также:



## В этом разделе



## Перевыпуск сертификата для Kaspersky Security Center Web Console

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Kaspersky Security Center Web Console равен 397 дням. Вы можете заменить существующий сертификат, полученный от аккредитованного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Kaspersky Security Center Web Console.

Если вы уже используете самоподписанный сертификат, вы также можете перевыпустить его, обновив Kaspersky Security Center Web Console, используя стандартную процедуру в установщике (параметр **Обновить**).

Когда вы открываете Web Console, браузер информирует вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется, так как сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить или предотвратить это предупреждение, можно выполнить одно из следующих действий:

- Укажите пользовательский сертификат при его повторном выпуске (рекомендуемый вариант). Создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 112).
- Добавьте сертификат Web Console в список доверенных сертификатов браузера после перевыпуска сертификата. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

► *Чтобы выпустить новый сертификат при первой установке Kaspersky Security Center Web Console:*

1. Запустите установку Kaspersky Security Center Web Console (см. стр. 950).
2. На шаге **Пользовательский сертификат** мастера установки выберите **Сгенерировать новый сертификат** и нажмите на кнопку **Далее**.

3. Выполните все шаги мастера установки, пока не завершите установку.

   Новый сертификат для Kaspersky Security Center Web Console выписан со сроком действия 397 дней.

► *Чтобы перевыпустить просроченный сертификат Kaspersky Security Center Web Console:*

1. Запустите исполняемый файл ksc-web-console-<номер_версии>.<номер сборки>.exe под учетной записью с правами администратора.
2. В открывшемся окне мастера установки выберите язык и нажмите на кнопку **ОК**.
3. В окне приветствия выберите параметр **Перевыпуск сертификата** и нажмите на кнопку **Далее**.
4. На следующем шаге дождитесь завершения перенастройки Kaspersky Security Center Web Console и нажмите на кнопку **Готово**.

   Сертификат Kaspersky Security Center Web Console перевыпущен со сроком действия 397 дней.

Если вы используете Identity and Access Manager (см. стр. 972), вы также должны повторно выпустить все TLS-сертификаты для портов, которые используют Identity and Access Manager (см. стр. 946). В Kaspersky Security Center Web Console отображается уведомление об истечении срока действия сертификата. Следуйте инструкциям из уведомления.

## Замена сертификата для Kaspersky Security Center 14.2 Web Console

По умолчанию при установке Сервера Kaspersky Security Center 14.2 Web Console сертификат браузера для программы генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

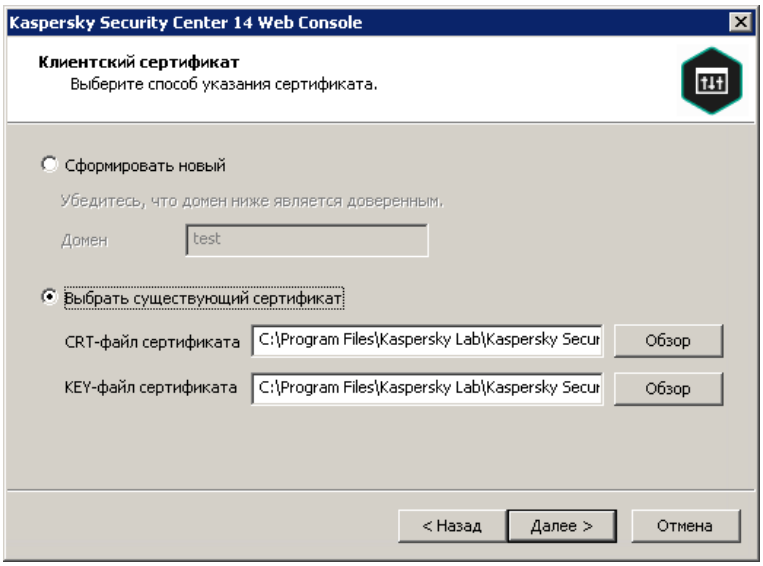
► *Чтобы заменить сертификат для Сервера Kaspersky Security Center 14.2 Web Console на пользовательский сертификат:*

1. Запустите на устройстве, на котором установлен Сервер Kaspersky Security Center 14.2 Web Console, исполняемый файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

   Запускается мастер установки.

2. На первой странице мастера выберите параметр **Обновить**.

3. На странице **Клиентский сертификат** выберите параметр **Выбрать существующий сертификат** и укажите путь к пользовательскому сертификату.




4. На последней странице мастера нажмите на кнопку **Изменить**, чтобы применить новые параметры.
5. После успешного завершения настройки программы нажмите кнопку **Готово**.

Kaspersky Security Center 14.2 Web Console работает с указанным сертификатом.

## Задание сертификатов для доверенных Серверов администрирования в Kaspersky Security Center 14.2 Web Console

Существующий сертификат Сервера администрирования автоматически заменяется новым до истечения срока действия сертификата. Вы также можете заменить существующий сертификат Сервера администрирования пользовательским сертификатом. При каждом изменении сертификата новый сертификат должен быть указан в параметрах программы Kaspersky Security Center 14.2 Web Console. Иначе Kaspersky Security Center 14.2 Web Console не сможет подключиться к Серверу администрирования.

Если Kaspersky Security Center 14.2 Web Console и Сервер администрирования установлены на одном устройстве, Kaspersky Security Center 14.2 Web Console получает новый сертификат автоматически. Если программа Kaspersky Security Center 14.2 Web Console установлена на другом устройстве, вы должны указать локальный путь к новому сертификату Сервера администрирования.

► *Чтобы задать новый сертификат для Сервера администрирования:*

1. На устройстве, на котором установлен Сервер администрирования, скопируйте файл сертификата, например, на запоминающее устройство.

   По умолчанию файл сертификата хранится в следующей папке:

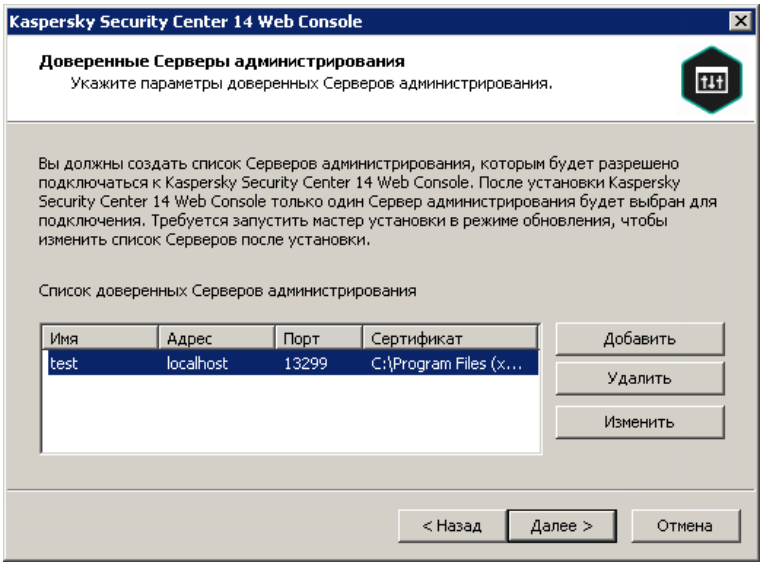
   - Для устройств с операционной системой Windows: %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.
   - Для устройств с операционной системой Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/.
2. На устройстве, на котором установлена программа Kaspersky Security Center 14.2 Web Console, поместите файл сертификата в локальную папку.
3. Запустите установочный файл ksc-web-console-<номер версии>.<номер сборки>.exe под учетной записью с правами администратора.

Запускается мастер установки.

4. На первой странице мастера выберите параметр **Обновить**.

   Следуйте далее указаниям мастера.

5. На странице мастера **Доверенные Серверы администрирования** выберите требуемый Сервер администрирования и нажмите на кнопку **Изменить**.




6. В открывшемся окне **Изменить Сервер администрирования** нажмите на кнопку **Обзор** кнопку и укажите путь к новому файлу сертификата, а, затем нажмите на кнопку **Обновить** для применения изменений.
7. На странице мастера **Все готово для изменения Kaspersky Security Center Web Console** нажмите на кнопку **Обновить**, чтобы начать обновление.
8. После успешного завершения настройки программы нажмите кнопку **Готово**.
9. Войдите (см. стр. 970) в Kaspersky Security Center 14.2 Web Console.

Kaspersky Security Center 14.2 Web Console работает с указанным сертификатом.

## См. также:

О сертификате Сервера администрирования.....111

## Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center 14.2 Web Console, вам необходимо предварительно преобразовать его в формат PEM с помощью любой кроссплатформенной утилиты на основе OpenSSL.

► *Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Windows:*

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
```

В результате вы получаете открытый ключ в виде файла .crt и закрытый ключ в виде защищенного парольной фразой файла .pem.

2. Убедитесь, что файлы .crt и .pem сгенерированы в той же папке, где хранится .pfx файл.
3. Если файл .crt или .pem содержит пакет атрибутов, удалите эти атрибуты с помощью любого удобного текстового редактора и сохраните файл.
4. Перезапустите службу Windows.
5. Kaspersky Security Center 14.2 Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center 14.2 Web Console (см. стр. 963).

► *Чтобы преобразовать сертификат из формата PFX в формат PEM в операционной системе Linux:*

1. В кроссплатформенной утилите на основе OpenSSL выполните следующие команды:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Убедитесь, что файл сертификата и закрытый ключ сгенерированы в той же папке, где хранится файл PFX.
3. Kaspersky Security Center 14.2 Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Не используйте одно и то же имя для входных и выходных файлов .pem.

   В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center 14.2 Web Console (см. стр. 963).

kaspersky

# Перенос данных в Kaspersky Security Center Linux или Kaspersky Security Center Cloud Console

В этом разделе описан перенос данных управляемых устройств и связанных с ними объектов (политик, задач, групп, тегов и других объектов) из Kaspersky Security Center Windows в Kaspersky Security Center Linux или Kaspersky Security Center Cloud Console.

## В этом разделе



## О переносе данных в Kaspersky Security Center Cloud Console

Вы можете выполнить перенос данных из программы Kaspersky Security Center Web Console в Kaspersky Security Center Cloud Console вручную. После этого вы получаете доступ к Серверу администрирования и системе управления базами данных (СУБД), которые размещены в инфраструктуре "Лаборатории Касперского". Вам не нужен физический сервер или СУБД: и то, и другое обслуживается за вас специалистами "Лаборатории Касперского".

Вы можете перенести данные управляемых устройств с операционными системами Windows, Linux или macOS под управление Kaspersky Security Center Cloud Console. Если в вашей сети есть иерархия Серверов администрирования, вы можете сохранить ее в Kaspersky Security Center Cloud Console. Кроме того, вы можете перенести:

- Задачи и политики управляемых программ.
- Глобальные задачи (см. стр. 1109)
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги (см. стр. 1159), назначенные устройствам, данные которых вы переносите.

После завершения переноса данных вы сможете управлять устройствами с помощью Kaspersky Security Center Cloud Console. При этом переносимые объекты сохраняются, а Агент администрирования переустанавливается на все управляемые устройства.

Информацию о том, как выполнить перенос данных, и список предварительных требований см. в *справке Kaspersky Security Center Cloud Console https://click.kaspersky.com/?hl=ru&link=online_help&pid=KSC&version=1.0.0&helpid=186799*.

## О переносе данных в программу Kaspersky Security Center Linux

В этом разделе представлена информация о способах переноса данных из программы Kaspersky Security Center Windows в Kaspersky Security Center Linux.

С помощью функции переноса данных вы можете перенести текущие объекты (политики, задачи, группы, теги и другие объекты) из Kaspersky Security Center Windows под управление Kaspersky Security Center Linux. Для переноса всех объектов используйте мастер переноса данных. Этот мастер сохраняет выбранные объекты в ZIP-файл и позволяет импортировать объекты из файла в Kaspersky Security Center Linux. Кроме мастера,

есть другой способ переноса текущих объектов, но этот способ позволяет переносить только политики и задачи. Вы можете перенести выбранные политики и задачи с помощью файла KLP.

Обратите внимание, что импорт с помощью мастера переноса данных не поддерживается в текущей версии Kaspersky Security Center Linux. Возможность импорта объектов данных будет добавлена в следующих версиях Kaspersky Security Center Linux. В текущей версии вы можете перенести определенные политики и задачи.

В текущей версии Kaspersky Security Center Linux вы можете переместить управляемые устройства под управление Kaspersky Security Center Linux либо с помощью утилиты klmover https://support.kaspersky.com/KSCLinux/14/ru-RU/227839.htm, либо установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки https://support.kaspersky.com/KSCLinux/14/ru-RU/236055.htm. Задача удаленной установки должна выполняться с помощью точки распространения с операционной системой Windows. Для этого назначьте устройство с операционной системой Windows в качестве точки распространения (см. стр. 1266) и включите параметр **Средствами операционной системы с помощью точек распространения** в задаче удаленной установки.

Вы можете перенести управляемые устройства и данные в Kaspersky Security Center Linux следующими способами:

- Перенесите управляемые устройства и данные с помощью мастера переноса данных (см. стр. 969):
  - Перенос данных без иерархии Серверов администрирования

    Выберите этот параметр, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux не выстроены в иерархию. Вам нужно будет перенести файл экспорта в Kaspersky Security Center Linux на съемном диске, по электронной почте, через общие папки или любым другим удобным способом. Вы управляете процессом переноса данных с помощью двух экземпляров Kaspersky Security Center Web Console, одного экземпляра Kaspersky Security Center Windows и другого Kaspersky Security Center Linux.
  - Перенос данных с использованием иерархии Серверов администрирования

    Выберите этот параметр, если Сервер администрирования Kaspersky Security Center Windows является подчиненным по отношению к Серверу администрирования Kaspersky Security Center Linux. Файл экспорта будет автоматически передан в Kaspersky Security Center Linux. Вы управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. В этом случае создайте иерархию заранее, до начала переноса данных.
- Экспортируйте определенные задачи (см. стр. 1119) из Kaspersky Security Center Windows, а затем импортируйте задачи (см. стр. 1120) в Kaspersky Security Center Linux.
- Экспортируйте определенные политики (см. стр. 1179) из Kaspersky Security Center Windows, а затем импортируйте политики (см. стр. 1180) в Kaspersky Security Center Linux. Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

## См. также:

Перенос данных в программу Kaspersky Security Center Linux .....969

kaspersky

# Перенос данных в программу Kaspersky Security Center Linux

В этом разделе описан перенос данных управляемых устройств и связанных с ними объектов (см. стр. 967) (политик, задач, групп, тегов и других объектов) из Kaspersky Security Center Windows в Kaspersky Security Center Linux с помощью мастера переноса данных. Вы можете включить одну группу администрирования в область переноса данных, чтобы восстановить эту группу администрирования в Kaspersky Security Center Linux. После завершения переноса данных все управляемые устройства и связанные с ними объекты будут управляться вашим экземпляром Kaspersky Security Center Linux.

Обратите внимание, что импорт с помощью мастера переноса данных не поддерживается в текущей версии Kaspersky Security Center Linux. Возможность импорта объектов данных будет добавлена в следующих версиях Kaspersky Security Center Linux. В текущей версии вы можете перенести определенные политики и задачи (см. стр. 967).

В текущей версии Kaspersky Security Center Linux вы можете переместить управляемые устройства под управление Kaspersky Security Center Linux либо с помощью утилиты klmover https://support.kaspersky.com/KSCLinux/14/ru-RU/227839.htm, либо установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки https://support.kaspersky.com/KSCLinux/14/ru-RU/236055.htm. Задача удаленной установки должна выполняться с помощью точки распространения с операционной системой Windows. Для этого назначьте устройство с операционной системой Windows в качестве точки распространения (см. стр. 1266) и включите параметр **Средствами операционной системы с помощью точек распространения** в задаче удаленной установки.

### Что можно перенести

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых программ.
- Глобальные задачи (см. стр. 1109).
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги (см. стр. 1159), назначенные устройствам, данные которых вы переносите.

### Прежде чем начать

Прочитайте общую информация о переносе данных в Kaspersky Security Center Linux (см. стр. 967). Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux.

### Мастер переноса данных

► *Чтобы экспортировать управляемые устройства и связанные объекты с помощью мастера переноса данных:*

1. В зависимости от того, выстроены ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center Linux, выполните одно из следующих действий:
   - Если Серверы выстроены в иерархию, где Kaspersky Security Center Linux является главным Сервером администрирования, а Kaspersky Security Center Windows – подчиненным Сервером

администрирования, откройте Kaspersky Security Center14.2 Web Console и переключитесь на Сервер Kaspersky Security Center Windows.

- Если Серверы не выстроены в иерархию, откройте Kaspersky Security Center 14.2 Web Console, подключенную к Kaspersky Security Center Windows.

2. В главном окне программы перейдите в раздел **Операции** → **Перенос данных**.
3. Выберите **Перенос данных в Kaspersky Security Center Linux** чтобы запустить мастер, и следуйте его шагам.
4. Выберите группу или подгруппу администрирования, которую вы хотите экспортировать. Обратите внимание, что в выбранной группе или подгруппе администрирования должно быть не более 10 000 устройств.
5. Выберите управляемые программы, задачи и политики которых будут экспортированы. Выберите только те программы, которые поддерживаются Kaspersky Security Center Linux. Объекты неподдерживаемых программ все равно будут экспортированы, но не будут работать.
6. Используйте ссылки слева, чтобы выбрать глобальные задачи, выбранные устройства и отчеты для экспорта. Ссылка **Групповые объекты** позволяет исключить из экспорта роли пользователей, внутренних пользователей и группы безопасности, а также пользовательские категории программ.
7. Файл экспорта (ZIP-архив) создан. Если Серверы выстроены в иерархию, файл экспорта сохраняется во временную папку на Сервере Kaspersky Security Center 14.2 Web Console. Иначе файл экспорта загрузится на ваше устройство.
8. Для переноса данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта.

# Вход в программу Kaspersky Security Center 14.2 Web Console и выход из нее

Вы можете войти в Kaspersky Security Center 14.2 Web Console после установки Сервера администрирования и Kaspersky Security Center Web Console (см. стр. 950). Вы должны знать веб-адрес Сервера администрирования и номер порта, указанный во время установки (см. стр. 950) (по умолчанию используется порт 8080). В вашем браузере JavaScript должен быть включен.

Войти в Kaspersky Security Center 14.2 Web Console можно одним из следующих способов:

- Используя доменную аутентификацию (см. стр. 979).

  Если вы выберете этот способ, убедитесь, что Опрос Active Directory (см. стр. 1058) активирован и доменные пользователи добавлены на Сервер администрирования.

- Указав имя учетной записи и пароль администратора.

**Вход с использованием доменной аутентификации**

► *Чтобы войти в Kaspersky Security Center 14.2 Web Console, используя доменную аутентификацию:*

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

   Отобразится страница входа в программу.

2. Если вы добавили несколько доверенных Серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

   - Нажмите на кнопку **Доменная аутентификация.**
   - Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер с использованием доменной аутентификации:

     a. Нажмите на кнопку **Дополнительные параметры**.

     b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера (см. стр. 989).

     c. Нажмите на кнопку **Доменная аутентификация**.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center 14.2 Web Console и использовать ее для работы с Kaspersky Security Center.

**Вход с указанием имени учетной записи и пароля администратора**

► *Чтобы войти в Kaspersky Security Center 14.2 Web Console, указав имя учетной записи и пароль администратора:*

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

   Отобразится страница входа в программу.

2. Если вы добавили несколько доверенных Серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, список Серверов администрирования не отображается.

3. Выполните одно из следующих действий:

   - Для входа на Сервер администрирования:

     a. Введите имя пользователя и пароль локального администратора.

     b. Нажмите на кнопку **Войти**.

   - Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:

     a. Нажмите на кнопку **Дополнительные параметры**.

     b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера (см. стр. 989).

     c. Введите имя пользователя и пароль администратора, имеющего права на виртуальном Сервере администрирования.

     d. Нажмите на кнопку **Войти**.

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center 14.2 Web Console и использовать ее для работы с Kaspersky Security Center.

**Выход**

► *Чтобы выйти из Kaspersky Security Center 14.2 Web Console,*

в главном меню перейдите в параметры своей учетной записи и выберите **Выход**.

Программа Kaspersky Security Center 14.2 Web Console закрыта, отображается страница входа в программу.

# Identity and Access Manager в Kaspersky Security Center 14.2 Web Console

В этом разделе представлена информация о Identity and Access Manager (далее также IAM).

## В этом разделе



## О компоненте Identity and Access Manager

*Identity and Access Manager* (далее также IAM) – это компонент Kaspersky Security Center 14.2 Web Console, позволяющий использовать единый вход (Single Sign-on, SSO) между Kaspersky Security Center 14.2 Web Console и веб-интерфейсом Kaspersky Industrial CyberSecurity for Networks. IAM использует протокол OAuth 2.0 для авторизации Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center 14.2 Web Console.

В этом случае программа Kaspersky Industrial CyberSecurity for Networks, доступ к которой вы получаете через Kaspersky Security Center 14.2 Web Console, называется *сервером ресурсов*, Kaspersky Security Center 14.2 Web Console и веб-интерфейс Kaspersky Industrial CyberSecurity for Networks называются *клиенты OAuth 2.0*. Сервер ресурсов – это программа, которая работает с несколькими пользователями и требует авторизации. Клиент использует *токен* для авторизации на сервере ресурсов. Токен – это уникальная последовательность байтов. По истечении срока действия токена он автоматически перевыпускается. IAM действует как единый сервер авторизации для нескольких клиентов OAuth 2.0.

Вы можете установить IAM при установке Kaspersky Security Center 14.2 Web Console. Вы можете включить его позже в любой момент в параметрах Kaspersky Security Center 14.2 Web Console. Если Сервер Kaspersky Industrial CyberSecurity или веб-интерфейс Kaspersky Industrial CyberSecurity установлены на устройстве, управляемым тем же Сервером администрирования, IAM обнаруживает эту программу, и в Kaspersky Security Center 14.2 Web Console отображается уведомление об этом. Вы можете зарегистрировать Kaspersky Industrial CyberSecurity for Networks, а затем использовать SSO как для Kaspersky Security Center 14.2 Web Console, так и для веб-интерфейса Kaspersky Industrial CyberSecurity for Networks.

Если вы выйдете из Kaspersky Security Center 14.2 Web Console, ваш сеанс в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks завершится, и вам придется снова войти в Kaspersky Security Center 14.2 Web Console.

## См. также:



# Включение Identity and Access Manager: сценарий

### Предварительные требования

Перед началом работы убедитесь, что у вас есть доступ к Kaspersky Industrial CyberSecurity for Networks версии 3.1 или новее.

### Этапы

Включение Identity and Access Manager (также называемого IAM) происходит поэтапно:

a. **Проверка необходимых портов**

   Убедитесь, что на устройстве, на котором установлена программа Kaspersky Security Center 14.2 Web Console, открыты порты 3333, 4004 и 4444. Эти порты необходимы для использования OAuth 2.0. Вы можете изменить номера портов по умолчанию в окне параметров Kaspersky Security Center 14.2 Web Console (см. стр. 974).

   Кроме портов 3333, 4004 и 4444, Kaspersky Security Center 14.2 Web Console также использует порты 4445, 2444 и 2445 для различных целей (см. стр. 946).

b. **Установка Identity and Access Manager**

   Во время установки (см. стр. 950) Kaspersky Security Center 14.2 Web Console укажите, что вы хотите установить Identity and Access Manager. Если вы этого не сделали, запустите еще раз мастер установки Kaspersky Security Center 14.2 Web Console.

c. **Настройка Identity and Access Manager**

   В окне параметров Kaspersky Security Center 14.2 Web Console (см. стр. 974) убедитесь, что переключатель **Identity and Access Manager (IAM)** включен. Также укажите DNS-имя устройства, на котором установлена программа Kaspersky Security Center 14.2 Web Console: клиентские программы будут подключаться к этому устройству.

d. **Указание параметров токена**

   В окне параметров Kaspersky Security Center 14.2 Web Console (см. стр. 974) укажите время жизни токенов и время ожидания авторизации, которые будет использовать Identity and Access Manager. Вы

можете использовать значения по умолчанию или указать свои значения в соответствии с вашими требованиями.

e. **Предоставление сертификатов**

Если вы предпочитаете использовать сертификаты, сгенерированные Сервером администрирования, то в окне параметров Kaspersky Security Center 14.2 Web Console (см. стр. 974) загрузите корневые сертификаты для портов, используемых IAM, и раздайте их рабочим станциям пользователей Kaspersky Security Center 14.2 Web Console. В противном случае браузеры пользователей будут отображать сообщения об ошибках при попытке подключения к Kaspersky Security Center 14.2 Web Console.

f. **Регистрация Серверов Kaspersky Industrial CyberSecurity for Networks и веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks**

При установке IAM в Kaspersky Security Center 14.2 Web Console отображается сообщение о том, что Сервер Industrial CyberSecurity for Networks (или несколько Серверов) и один или несколько веб-интерфейсов Kaspersky Industrial CyberSecurity for Networks ожидают регистрации. Нажмите на это сообщение, чтобы зарегистрировать (см. стр. 975) Сервер Kaspersky Industrial CyberSecurity for Networks Server (или Серверы) и веб-интерфейс (или веб-интерфейсы).

**Результаты**

После завершения этого сценария вы сможете использовать SSO и IAM https://support.kaspersky.com/KICSforNetworks/3.1/ru-RU/110348.htm для Kaspersky Industrial CyberSecurity for Networks и Kaspersky Security Center 14.2 Web Console.

## Настройка Identity and Access Manager в Kaspersky Security Center 14.2 Web Console

► *Чтобы настроить Identity and Access Manager в соответствии с вашими требованиями:*

1. В главном окне программы перейдите в раздел **Параметры консоли → Интеграция**.
2. В разделе **Identity and Access Manager** убедитесь, что Identity and Access Manager включен.
3. Перейдите по ссылке **Параметры** в **Сетевое имя устройства Identity and Access Manager**.
4. Укажите DNS-имя устройства, на котором вы установили Identity and Access Manager. Клиентские программы будут подключаться к этому устройству.
5. Если хотите, измените параметры токена по умолчанию (см. стр. 976), параметры сертификата (см. стр. 978) и номера портов (см. стр. 946) нажав на ссылку **Параметры** под соответствующей группой параметров.

Identity and Access Manager включен и работает в соответствии с вашими требованиями.

### См. также:

Включение Identity and Access Manager: сценарий.....973

kaspersky

# Регистрация веб-интерфейса Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center 14.2 Web Console

Чтобы начать работу с веб-интерфейсом Kaspersky Industrial CyberSecurity for Networks через Kaspersky Security Center 14.2 Web Console, необходимо предварительно зарегистрировать его в Kaspersky Security Center 14.2 Web Console.

Чтобы зарегистрировать веб-интерфейс Kaspersky Industrial CyberSecurity for Networks:

1. Убедитесь, что сделано следующее:
   - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks (см. стр. 1037).

     Вы можете сделать это позже, ожидая синхронизации Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования.
   - Вы завершили сценарий подготовки к использованию технологии единого входа (SSO).
   - Необходимые параметры в веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks заданы на странице Kaspersky Security Center. Подробную информацию см. в онлайн-справке Kaspersky Industrial CyberSecurity for Networks.
   - Вы вошли в Kaspersky Security Center 14.2 Web Console под учетной записью администратора.
   - IAM настроен (см. стр. 974).
2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:
   a. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
   b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.
   c. Нажмите на кнопку **Переместить в группу**.
   d. В иерархии групп администрирования установите флажок рядом с группой Управляемые устройства.
   e. Нажмите на кнопку **Переместить**.
3. Перейдите к свойствам устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.
4. На странице свойств устройства в разделе **Общие**, выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.
5. В окне свойств устройства выберите раздел **Программы**.
6. В разделе **Программы** выберите Агент администрирования.
7. Если текущий статус программы *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас, пока ждете.
8. В главном окне программы перейдите в раздел **Параметры консоли** → **Интеграция**.

   В поле **Запросы на регистрацию**, отображается один ожидающий запрос.
9. Перейдите по ссылке **Параметры**, расположенной ниже поля **Запросы на регистрацию**.

10. В открывшемся списке зарегистрированных клиентов установите флажок рядом с названием того Сервера Kaspersky Industrial CyberSecurity for Networks, который имеет статус *Ожидает применения*, а затем нажмите на кнопку **Одобрить**.

    Если вы не хотите регистрировать Сервер Kaspersky Industrial CyberSecurity for Networks, вы можете нажать на кнопку Отклонить и вернуться к этому списку позже.

    После того, как вы нажмете на кнопку **Одобрить**, статус меняется на *Одобрено*, а затем на *Готов*. Если статус не поменялся, вы можете нажать на кнопку Обновить.

11. Закройте список зарегистрированных клиентов и убедитесь, что значение в поле **Зарегистрированные клиенты** увеличилось.

12. Чтобы добавить веб-виджет Kaspersky Industrial CyberSecurity for Networks на панель управления:

    a. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.

    b. На панели мониторинга нажмите на кнопку **Добавить или восстановить веб-виджет**.

    c. В появившемся веб-виджете нажмите на кнопку **Другое**.

    d. Выберите виджет Kaspersky Industrial CyberSecurity for Networks.

    Теперь вы можете перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks по ссылке в веб-виджете.

После завершения процедуры регистрации появится новая кнопка **Kaspersky Security Center**, которая отображается на странице входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks. Вы можете нажать на эту кнопку, чтобы войти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks под своими учетными данными Kaspersky Security Center.

## Время жизни токенов и время ожидания авторизации для Identity and Access Manager

При настройке компонента Identity and Access Manager (далее также IAM) необходимо указать параметры времени жизни токена и время ожидания авторизации. Параметры по умолчанию разработаны с учетом одновременно и стандартов безопасности, и нагрузки на Сервер. Вы можете менять эти параметры в соответствии с политиками вашей организации.

IAM автоматически повторно выпускает токен, когда срок его действия истекает.

В таблице ниже перечислены параметры времени жизни токена по умолчанию.

*Таблица 84. Параметры времени жизни токена*

| Токен | Время жизни по умолчанию (в секундах) | Описание |
|---|---|---|
| **Идентификационный токен (id_token)** | 86400 | Идентификационный токен, используемый клиентом OAuth 2.0 (то есть Kaspersky Security Center 14.2 Web Console или веб-интерфейсом Kaspersky Industrial CyberSecurity). IAM отправляет идентификатор токена, который содержит информацию о пользователе (то есть профиль пользователя) клиенту. |
| **Токен доступа (access_token)** | 86400 | Токен доступа, используемый клиентом OAuth 2.0 для доступа к серверу ресурсов от имени владельца ресурса, определенного IAM. |
| **Обновить токен (refresh_token)** | 172800 | Клиент OAuth 2.0 использует этот токен для повторной выдачи идентификационного токена и токена доступа. |

В таблице ниже приведено время ожидания для auth_code и login_consent_request.

*Таблица 85. Параметры времени ожидания авторизации*

| Параметр | Время ожидания по умолчанию (в секундах) | Описание |
|---|---|---|
| **Код авторизации (auth_code)** | 3600 | Время ожидания обмена кода токена. Клиент OAuth 2.0 отправляет этот код на сервер ресурсов и взамен получает токен доступа. |
| **Время ожидания запроса на вход (login_consent_request)** | 3600 | Время ожидания для делегирования прав пользователя клиенту OAuth 2.0. |

Для получения дополнительной информации о токенах см. веб-сайт OAuth https://www.oauth.com.

## См. также:

Включение Identity and Access Manager: сценарий.....973

kaspersky

## Загрузка и распространение IAM-сертификатов

По умолчанию Identity and Access Manager использует сертификаты, созданные Сервером администрирования, для предоставления доступа браузерам к Kaspersky Security Center 14.2 Web Console. Вы также можете использовать пользовательские сертификаты. Какой бы сертификат вы ни использовали, вы должны убедиться, что все рабочие станции, с которых пользователи Kaspersky Security Center 14.2 Web Console обращаются к Kaspersky Security Center 14.2 Web Console, доверяют этому сертификату.

► *Чтобы загрузить и распространить сертификаты:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Интеграция**.
2. Для каждого сертификата нажмите на ссылку **Настройки** под соответствующей группой параметров, и выполните одно из следующих действий:
   - Если вы хотите использовать сертификат, сгенерированный Сервером администрирования при установке Kaspersky Security Center 14.2 Web Console:
     1. Выберите **Сертификат, созданный Сервером администрирования** в открывшемся окне свойств сертификата.
     2. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel.
     3. Распространите загруженный сертификат на все рабочие станции, с которых пользователи Kaspersky Security Center 14.2 Web Console получают доступ к Kaspersky Security Center 14.2 Web Console.
   - Если у вас есть сертификат, который вы хотите использовать:
     1. Выберите **Пользовательский TLS-сертификат** в открывшемся окне свойств сертификата.
     2. Выберите файл сертификата и закрытый ключ.
     3. Нажмите на кнопку **ОК**.
     4. Распространите сертификат на все рабочие станции, с которых пользователи получают доступ к Kaspersky Security Center 14.2 Web Console или веб-интерфейсу Kaspersky Industrial CyberSecurity.

Сертификаты предоставляют пользователям доступ к Kaspersky Security Center 14.2 Web Console и веб-интерфейсу Kaspersky Industrial CyberSecurity.

Вам необходимо своевременно перевыпустить все сертификаты. Сертификаты, сгенерированные Сервером администрирования, необходимо заново сгенерировать вручную. Сертификаты, сгенерированные установщиком (см. стр. 950) Kaspersky Security Center 14.2 Web Console, необходимо повторно сгенерировать с помощью установщика.

### См. также:

Включение Identity and Access Manager: сценарий.....973

## Отключение Identity and Access Manager

Вы можете выключить Identity and Access Manager (IAM).

► *Чтобы отключить IAM,*

В окне параметров Kaspersky Security Center 14.2 Web Console установите переключатель IAM в неактивное положение.

Вы можете включить IAM позже в любое время.

Если вы обновите Kaspersky Security Center 14.2 Web Console через установщик и укажете, что вы не хотите устанавливать IAM, то Kaspersky Security Center 14.2 Web Console будет обновлен, а IAM не будет установлен. С вашего устройства будут удалены: вся информация об интеграции с Kaspersky Industrial CyberSecurity for Networks, файлы конфигурации IAM и файлы журналов событий.

### См. также:

Включение Identity and Access Manager: сценарий.....973

# Настройка доменной аутентификации с использованием протоколов NTLM и Kerberos

Kaspersky Security Center позволяет использовать доменную аутентификацию в OpenAPI по протоколам NTLM и Kerberos. Использование доменной аутентификации позволяет пользователю Windows включить безопасную аутентификацию в Kaspersky Security Center 14.2 Web Console без повторного ввода пароля в корпоративной сети (единый вход).

Доменная аутентификация в OpenAPI по протоколу Kerberos имеет следующие ограничения:

- Пользователь Kaspersky Security Center 14.2 Web Console должен пройти аутентификацию в Active Directory по протоколу Kerberos. У пользователя должен быть действующий билет на получение билетов Kerberos (далее также TGT). TGT выдается автоматически при аутентификации в домене.
- Вы должны настроить аутентификацию Kerberos в браузере. Подробнее см. в документации используемого вами браузера.

Если вы хотите использовать доменную аутентификацию с использованием протоколов Kerberos, ваша сеть должна соответствовать следующим условиям:

- Сервер администрирования должен запускаться под доменной учетной записью.
- Сервер Kaspersky Security Center Web Console установлен на том же устройстве, что и Сервер администрирования.
- Для учетной записи Сервера администрирования необходимо указать следующие имена субъектов службы (SPN):
  - "http/<server.fqnd.name>"
  - "http/<server>"

Здесь <server> – сетевое имя устройства Сервера администрирования, <server.fqnd.name> – полное доменное имя устройства Сервера администрирования.

- При подключении через Консоль администрирования или Kaspersky Security Center Web Console необходимо указывать адрес Сервера администрирования точно так же, как адрес, для которого зарегистрировано имя субъекта-службы (SPN). Вы можете указать либо <serverhost.find.name> или <serverhost>.
- Для входа без пароля служба браузера, в котором открыта Kaspersky Security Center Web Console, должна работать под доменной учетной записью.

Протоколы Kerberos и NTLM поддерживаются только в OpenAPI для Kaspersky Security Center. Эти протоколы не поддерживаются в OpenAPI для Kaspersky Security Center Linux.

# Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования Kaspersky Security Center.

## В этом разделе

kaspersky

# Настройка параметров подключения Kaspersky Security Center 14.2 Web Console к Серверу администрирования

► *Чтобы задать порты подключения к Серверу администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Порты подключения**.

Будут отображены основные параметры подключения к выбранному Серверу Администрирования.

Консоль администрирования подключена к Серверу администрирования через SSL-порт TCP 13291. Этот же порт может использоваться объектами автоматизации klakaut.

Порт TCP 14000 может использоваться для подключения Консоли администрирования, точек распространения, подчиненных Серверов администрирования и объектов автоматизации утилиты klakaut, а также для получения данных с клиентских устройств.

SSL-порт TCP 13000 могут использовать только Агент администрирования, подчиненный Сервер и главный Сервер администрирования, размещенный в демилитаризованной зоне. В некоторых случаях может быть необходимо подключение Консоли администрирования по SSL-порту 13000:

- если предпочтительно использовать один и тот же SSL-порт как для Консоли администрирования, так и для других активностей (для получения данных с клиентских устройств, подключения точек распространения, подключения подчиненных Серверов администрирования);
- если объект автоматизации утилиты klakaut подключается к Серверу администрирования не напрямую, а через точку распространения, размещенную в демилитаризованной зоне.

## См. также:

Порты, используемые Kaspersky Security Center.....98

# Просмотр журнала подключений к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

► *Чтобы настроить регистрацию событий подключения к Серверу администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Порты подключения**.
3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

kaspersky

# Настройка параметров доступа Сервера администрирования к интернету

Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых программ "Лаборатории Касперского".

► *Чтобы указать параметры доступа Сервера администрирования к интернету:*

1. В главном меню нажмите на значок параметров (  ) рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Параметры доступа к сети интернет**.
3. Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

   - **Адрес**

     Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

   - **Номер порта**

     Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

   - **Не использовать прокси-сервер для локальных адресов**

     При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

   - **Аутентификация на прокси-сервере**

     Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

     Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

   - **Имя пользователя**

     Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

   - **Пароль**

     Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки (см. стр. 1009).

kaspersky

## Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программы вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые. Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий Kaspersky Event Log. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления.

► *Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Хранение событий**. Укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **Сохранить**.

Также можно изменить параметры любой задачи, чтобы сохранять события, связанные с ходом выполнения задачи, или сохранять только результаты выполнения задачи. Таким образом вы уменьшаете количество событий в базе данных, увеличиваете скорость работы сценариев, связанных с анализом таблицы событий в базе данных, и снижаете риск вытеснения критических событий большим количеством событий.

### См. также:


О блокировке частых событий ..... 1438

Сценарий: Настройка защиты сети ..... 400


## Параметры подключения устройств с защитой на уровне UEFI

*Устройство с защитой на уровне UEFI* – это устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы безопасности. Kaspersky Security Center поддерживает управление такими устройствами.

► *Чтобы изменить параметры подключения устройств с защитой на уровне UEFI:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Дополнительные порты**.
3. Измените требуемые параметры:
   - **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

     Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

   - **Порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**

     Вы можете изменить номер порта, если установлен флажок **Открыть порт для устройств с защитой на уровне UEFI и устройств с KasperskyOS**. По умолчанию установлен порт 13294.
4. Нажмите на кнопку **Сохранить**.

Устройства с защитой на уровне UEFI могут подключаться к Серверу администрирования.

# Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

**Добавление подчиненного Сервера администрирования (выполняется с будущим главным Сервером администрирования)**

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

► *Чтобы добавить Сервер администрирования, доступный для подключения через Kaspersky Security Center 14.2 Web Console, в качестве подчиненного Сервера:*

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. На будущем главном Сервере администрирования нажмите на значок параметров ( ).
3. На открывшейся странице свойств выберите закладку **Серверы администрирования**.
4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.
5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования.
6. На первой странице мастера заполните следующие поля:
   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".

   - **Адрес подчиненного Сервера администрирования (необязательно)**

     Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

   - **SSL-порт Сервера администрирования**

Укажите номер SSL-порта главного Сервера администрирования. По умолчанию установлен порт 13000.

- **API-порт Сервера администрирования**

  Укажите номер порта главного Сервера администрирования для получения соединений через OpenAPI. По умолчанию установлен порт 13299.

- **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**

  Выберите этот параметр, если подчиненный Сервер администрирования находится в демилитаризованной зоне (DMZ).

  Если выбран этот параметр, главный Сервер администрирования инициирует подключение к подчиненному Серверу администрирования. Иначе подчиненный Сервер администрирования инициирует подключение к главному Серверу администрирования.

1. Задайте параметры подключения:
   - Введите адрес будущего главного Сервера администрирования.
   - Если будущий подчиненный Сервер администрирования использует прокси-сервер, введите адрес прокси-сервера и учетные данные пользователя для подключения к прокси-серверу.
2. Введите учетные данные пользователя, имеющего права доступа на будущий подчиненный Сервер администрирования.

   Убедитесь, что двухэтапная проверка выключена для указанной вами учетной записи. Если для этой учетной записи включена двухэтапная проверка, то можно создать иерархию только из будущего подчиненного Сервера (см. инструкции ниже). Это известное ограничение (см. стр. 1507).

Если параметры соединения верны, устанавливается соединение с будущим подчиненным Сервером и строится иерархия "главный/подчиненный". Если подключение не удалось, проверьте параметры подключения или укажите сертификат будущего подчиненного Сервера (см. стр. 111) вручную.

Соединение также может не состояться из-за того, что будущий подчиненный Сервер выполняет аутентификацию с помощью самоподписанного сертификата, автоматически сгенерированного Kaspersky Security Center. В результате браузер может заблокировать загрузку самоподписанного сертификата. В этом случае можно выполнить одно из следующих действий:

- Для будущего подчиненного Сервера создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 112).
- Добавьте самоподписанный сертификат будущего подчиненного Сервера (см. стр. 111) в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат. Информацию о добавлении сертификата в список доверенных сертификатов см. в документации вашего браузера.

Соединение между главным и подчиненным Серверами администрирования устанавливается через порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

**Добавление подчиненного Сервера администрирования (выполняется с будущим подчиненным Сервером администрирования)**

Если вы не можете подключится к будущему подчиненному Серверу администрирования (например, потому что он был временно отключен или недоступен), вы все равно можете добавить подчиненный Сервер администрирования.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Kaspersky Security Center 14.2 Web Console, в качестве подчиненного Сервера:*

1. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

   Файл сертификата находится на будущем главном Сервере администрирования по адресу %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

   a. Нажмите на значок параметров ( ).

   b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на закладке **Общие**.

   c. Выберите параметр **Данный Сервер администрирования является подчиненным в иерархии**.

   d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

   e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

   f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   g. Если подключение к будущему подчиненному Серверу администрирования выполняется с помощью прокси-сервера, установить флажок **Использовать прокси-сервер** и задать параметры подключения.

   h. Нажмите на кнопку **Сохранить**.

Отношение "Главный Сервер – подчиненный Сервер" будет установлено. Главный Сервер начинает принимать подключение от подчиненного Сервера, используя порт 13000. Задачи и политики главного Сервера администрирования получены и применены. Подчиненный Сервер администрирования отображается на главном Сервере администрирования, в группе администрирования, в которую он был добавлен.

## См. также:


Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне .142

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования .....141

Порты, используемые Kaspersky Security Center.....98

kaspersky

## Просмотр списка подчиненных Серверов администрирования

► *Чтобы просмотреть список подчиненных (включая виртуальные) Серверов администрирования:*

В главном меню нажмите на имя Сервера администрирования, которое находится рядом со значком параметров (  ).

Отобразится раскрывающийся список подчиненных (включая виртуальные) Серверов администрирования.

Вы можете перейти на любой из этих Серверов администрирования, нажав на его имя.

Группы администрирования тоже отображаются, но они неактивны и недоступны для управления в этом меню.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Kaspersky Security Center 14.2 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center 14.2 Web Console.
- Используйте Kaspersky Security Center 14.2 Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования (см. стр. 984), на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center 14.2 Web Console.
- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу (см. стр. 674).

## Удаление иерархии Серверов администрирования

Если вам больше не нужна иерархия Серверов администрирования, вы можете отключить их от этой иерархии.

► *Чтобы удалить иерархию Серверов администрирования:*

1. В главном меню нажмите на значок параметров (  ) рядом с именем главного Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.
4. В меню выберите пункт **Удалить**.
5. В открывшемся окне нажмите на кнопку **ОК** для подтверждения удаления подчиненного Сервера администрирования.

Бывший главный Сервер администрирования и бывший подчиненный Сервер администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

## Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (если необходимо).

Задача обслуживания Сервера администрирования не поддерживает MariaDB. Если эта СУБД используется в вашей сети, администраторам придется поддерживать MariaDB самостоятельно.

Задача Обслуживание Сервера администрирования создается автоматически при установке Kaspersky Security Center. Если задача Обслуживание Сервера администрирования удалена, вы можете создать ее вручную.

► *Чтобы создать задачу Обслуживание Сервера администрирования:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В окне мастера **Новая задача** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате созданная задача отобразится в списке задач. Для одного Сервера администрирования может выполняться только одна задача обслуживания Сервера администрирования. Если задача Обслуживание Сервера администрирования для Сервера уже создана, создание еще одной задачи Обслуживание Сервера администрирования невозможно.

kaspersky

## Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center 14.2 Web Console на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

► *Чтобы настроить интерфейс Kaspersky Security Center 14.2 Web Console в соответствии в соответствии с используемым в настоящее время набором функций:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** включите или выключите требуемые параметры.
3. Нажмите на кнопку **Сохранить**.

После этого в консоли отображаются разделы в главном меню в соответствии с включенными параметрами. Например,если включить параметр **Показать EDR-обнаружения**, раздел **Мониторинг и отчеты** → **Обнаружения** появится в главном меню.

# Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования (см. стр. 989);
- включение и выключение виртуальных Серверов администрирования (см. стр. 990);
- назначение администратора виртуального Сервера администрирования (см. стр. 991);
- смена Сервера администрирования для клиентских устройств (см. стр. 993);
- удаление виртуальных Серверов администрирования (см. стр. 994).

### В этом разделе



## Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования (см. стр. 169) и добавить их в группы администрирования.

► *Чтобы создать и добавить виртуальный Сервер администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Иерархия Серверов администрирования**.

3. Выберите группу администрирования, в которую вы хотите добавить виртуальный Сервер администрирования.
   Виртуальный Сервер администрирования будет управлять устройствами из выбранной группы (включая подгруппы).
4. В меню выберите пункт **Создать виртуальный Сервер администрирования**.
5. На открывшейся странице задайте свойства нового виртуального Сервера администрирования:
   - **Имя виртуального Сервера администрирования**
   - **Адреса подключения к Серверу администрирования**

     Вы можете указать имя или IP-адрес Сервера администрирования.
6. Из списка пользователей выберите администратора виртуального Сервера администрирования. Существующую учетную запись при необходимости можно изменить перед тем, как назначить ей роль администратора; можно также создать новую учетную запись.
7. Нажмите на кнопку **Сохранить**.

Новый виртуальный Сервер администрирования создан, добавлен в группу администрирования и отображается на закладке **Иерархия Серверов администрирования**.

Если вы подключены к главному Серверу администрирования в Kaspersky Security Center Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Kaspersky Security Center 14.2 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center 14.2 Web Console.
- Используйте Kaspersky Security Center 14.2 Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования (см. стр. 984), на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center 14.2 Web Console.
- Используйте Консоль администрирования на основе MMC для прямого подключения к виртуальному Серверу (см. стр. 674).

## Включение и выключение виртуального Сервера администрирования

Когда вы создаете виртуальный Сервер администрирования, он по умолчанию включается. Вы можете выключить или снова включить его в любое время. Выключение или включение виртуального Сервера администрирования равносильно выключению или включению физического Сервера администрирования.

► *Чтобы включить или выключить виртуальный Сервер администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Иерархия Серверов администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.
4. В строке меню нажмите на кнопку **Подключить/отключить виртуальный Сервер администрирования**.

Состояние виртуального Сервера администрирования изменяется на включено или выключено в зависимости от его предыдущего состояния. Обновленное состояние отображается рядом с именем Сервера администрирования.

## См. также:

Удаление виртуального Сервера администрирования ..... 994

## Назначение администратора виртуального Сервера администрирования

Если вы используете в своей организации виртуальные Серверы администрирования, вам может потребоваться назначить отдельного администратора для каждого виртуального Сервера администрирования. Например, это может быть полезно, когда вы создаете виртуальные Серверы администрирования для управления отдельными офисами или отделами вашей организации или если вы являетесь поставщиком услуг (MSP) и управляете своими тенантами с помощью виртуальных Серверов администрирования.

При создании виртуального Сервера администрирования он наследует список пользователей и все права пользователей главного Сервера администрирования. Если пользователь имеет права доступа к главному Серверу, этот пользователь также имеет права доступа к виртуальному Серверу. После создания вы самостоятельно настраиваете права доступа к Серверам. Если вы хотите назначить администратора только для виртуального Сервера администрирования, убедитесь, что у администратора нет прав доступа на главном Сервере администрирования.

Вы назначаете администратора виртуального Сервера администрирования, предоставляя права доступа администратору к виртуальному Серверу администрирования. Вы можете предоставить требуемые права доступа одним из следующих способов:

- Настройте права доступа для администратора вручную.
- Назначьте одну или несколько пользовательских ролей администратору.

Чтобы войти в Kaspersky Security Center Web Console (см. стр. 970), администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль. Kaspersky Security Center 14.2 Web Console выполняет аутентификацию администратора и открывает виртуальный Сервер администрирования, к которому у администратора есть права доступа. Администратор не может переключаться между Серверами администрирования.

### Предварительные требования

Убедитесь, что выполнены следующие условия:

- Виртуальный Сервер администрирования создан (см. стр. 989).
- На главном Сервере администрирования у вас создана учетная запись (см. стр. 766) для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право **Изменение списков управления доступом объектов** см. стр. 1191) в функциональной области **Общий функционал** → **Права пользователей**.

### Настройка прав доступа вручную

► *Чтобы назначить администратора виртуального Сервера администрирования:*

1. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:
   a. Нажмите на значок шеврона ( ) справа от текущего имени Сервера администрирования.

b. Выберите требуемый Сервер администрирования.

2. В главном меню нажмите на значок параметров ( ) рядом с именем главного Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

3. На закладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется единый список пользователей главного Сервера администрирования и текущего виртуального Сервера администрирования.

4. В списке пользователей выберите учетную запись администратора, которого вы хотите назначить для виртуального Сервера администрирования, и нажмите на кнопку **ОК**.

   Программа добавляет выбранного пользователя в список пользователей на закладку **Права доступа**.

5. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Права доступа**.

6. Настройте права администратора на виртуальном Сервере администрирования.

   Для успешной аутентификации администратор должен иметь следующие права:

   - право **Чтение** в функциональной области **Общий функционал → Базовая функциональность**;
   - право **Чтение** в функциональной области **Общий функционал → Виртуальные Серверы администрирования**.

Программа сохраняет измененные права пользователя в учетной записи администратора.

**Настройка прав доступа с помощью назначения пользовательских ролей**

Также вы можете предоставить права доступа администратору виртуального Сервера администрирования через пользовательскую роль. Например, это может быть полезно, если вы хотите назначить несколько администраторов на один и тот же виртуальный Сервер администрирования. В этом случае вы можете назначить учетным записям администраторов одну или несколько пользовательских ролей вместо того, чтобы настраивать одни и те же права для нескольких администраторов.

► *Чтобы назначить администратора виртуального Сервера администрирования, назначив ему пользовательские роли:*

1. На главном Сервере администрирования создайте пользовательскую роль (см. стр. 1222) и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования. Вы можете создать несколько ролей, например, если хотите разделить доступ к разным функциональным областям.
2. В главном меню переключитесь на требуемый виртуальный Сервер администрирования:

   a. Нажмите на значок шеврона ( ) справа от текущего имени Сервера администрирования.

   b. Выберите требуемый Сервер администрирования.

3. Назначьте новую роль или несколько ролей учетной записи администратора (см. стр. 797).

Программа назначает роль учетной записи администратора.

**Настройка прав доступа на уровне объекта**

В дополнение к назначению прав доступа на уровне функциональной области (см. стр. 1192), вы можете настроить доступ к определенным объектам (см. стр. 1216) на виртуальном Сервере администрирования, например, к определенной группе администрирования или задаче. Для этого переключитесь на виртуальный Сервер администрирования, а затем настройте права доступа в свойствах объекта.

См. также:

Удаление виртуального Сервера администрирования ..... 994

## Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером с помощью задачи **Смена Сервера администрирования**. После завершения задачи выбранные клиентские устройства будут под управлением указанного Сервера администрирования. Вы можете переключать управление устройством между следующими Серверами администрирования:

- главным Сервер администрирования и одним из его виртуальных Серверов администрирования;
- двумя виртуальными Серверами администрирования одного и того же главного Сервера администрирования.

► *Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для программы Kaspersky Security Center выберите тип задачи **Смена Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите Сервер администрирования, который вы хотите использовать для управления выбранными устройствами.
7. Задайте параметры учетной записи:
   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

     По умолчанию выбран этот вариант.
   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.
   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.
   - **Пароль**

     Пароль учетной записи, от имени которой будет запускаться задача.
8. Если вы включите параметр **Открыть окно свойств задачи после ее создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения

параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

9. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

10. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
11. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.
12. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

13. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

### См. также:

Управление виртуальными Серверами администрирования ..... 989

Сценарий: Настройка защиты сети ..... 400

## Удаление виртуального Сервера администрирования

При удалении виртуального Сервера администрирования все объекты, созданные на Сервере администрирования, включая политики и задачи, также будут удалены. Управляемые устройства из групп администрирования, которыми управлял виртуальный Сервер администрирования, будут удалены из групп администрирования. Чтобы вернуть устройства под управление Kaspersky Security Center, выполните опрос сети, а затем переместите найденные устройства из группы Нераспределенные устройства в группы администрирования.

► *Чтобы удалить виртуальный Сервер администрирования:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем главного Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Иерархия Серверов администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
4. В меню нажмите на кнопку **Удалить**.

Виртуальный Сервер администрирования удален.

### См. также:

Включение и выключение виртуального Сервера администрирования ..... 990

## Включение защиты учетной записи от несанкционированного изменения

Вы можете дополнительно включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

► *Чтобы включить или выключить защиту учетной записи от несанкционированного изменения:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите настроить защиту учетной записи от несанкционированного изменения.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Защита учетной записи** выберите параметр **Запросить аутентификацию для проверки разрешения на изменение учетных записей пользователей**, если вы хотите запрашивать учетные данные каждый раз при изменении параметров учетной записи. В противном случае выберите **Разрешить пользователям изменять эту учетную запись без дополнительной аутентификации**.
5. Нажмите на кнопку **Сохранить**.

Для учетной записи пользователя включена защита от несанкционированного изменения.

# Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Kaspersky Security Center 14.2 Web Console.

### В этом разделе



## Сценарий: Настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, программа сначала откроет окно

включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

**Предварительные требования**

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение проверки подлинности.

**Этапы**

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

a. **Установка приложения проверки подлинности на устройство**

   Вы можете установить Google Authenticator, Microsoft Authenticator или любое другое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени.

b. **Синхронизация времени приложения проверки подлинности и время устройства, на котором установлен Сервер администрирования**

   Убедитесь, что время, установленное в приложении проверки подлинности, синхронизировано со временем Сервера администрирования.

c. **Включение двухэтапной проверки и получение секретного ключа для своей учетной записи**

   Инструкции:

   Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для вашей учетной записи (см. стр. 703)

   Для Kaspersky Security Center 14.2 Web Console: Включение двухэтапной проверки для вашей учетной записи (см. стр. 999)

   После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

d. **Включение двухэтапной проверки для всех пользователей**

   Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

   Инструкции:

   Для Консоли администрирования на основе MMC: Включение двухэтапной проверки для всех пользователей (см. стр. 704)

   Для Kaspersky Security Center 14.2 Web Console: Включение двухэтапной проверки для всех пользователей (см. стр. 1000)

e. **Изменение имени издателя кода безопасности**

   Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

   Инструкции:

Для Консоли администрирования на основе MMC: Изменение имени издателя кода безопасности (см. стр. 707)

Для Kaspersky Security Center 14.2 Web Console: Изменение имени издателя кода безопасности (см. стр. 1003)

f. **Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку**

   При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

   Инструкции:

   Для Консоли администрирования на основе MMC: Исключение учетных записей из двухэтапной проверки (см. стр. 706)

   Для Kaspersky Security Center 14.2 Web Console: Исключение учетных записей из двухэтапной проверки (см. стр. 1001)

**Результаты**

После выполнения этого сценария:

- Двухэтапная проверка для вашей учетной записи включена.
- Двухэтапная проверка включена для всех учетных записей пользователей Сервера администрирования, кроме исключенных учетных записей пользователей.

## См. также:



## О двухэтапной проверке

Kaspersky Security Center предоставляет двухэтапную проверку для пользователей Kaspersky Security Center 14.2 Web Console. Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center 14.2 Web Console вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию (на стр. 979) для своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Чтобы получить одноразовый код безопасности, вы должны установить приложение проверки подлинности на своем компьютере или мобильном устройстве.

Код безопасности имеет идентификатор, называемый также *имя издателя*. Имя издателя кода безопасности используется в качестве идентификатора Сервера администрирования в приложении проверки подлинности. Вы можете изменить имя издателя кода безопасности. Имя издателя кода безопасности имеет значение по умолчанию, такое же, как имя Сервера администрирования. Имя издателя используется в качестве идентификатора Сервера администрирования в приложении проверки подлинности. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению проверки подлинности. Код безопасности является одноразовым и действует до 90 секунд (точное время может варьироваться).

Любой пользователь, для которого включена двухэтапная проверка, может повторно ввести свой секретный ключ. Когда пользователь выполняет аутентификацию с повторно выданным секретным ключом и использует

этот ключ для входа в программу, Сервер администрирования сохраняет новый секретный ключ для учетной записи пользователя. Если пользователь неправильно ввел новый секретный ключ, Сервер администрирования не сохраняет новый секретный ключ и оставляет текущий секретный ключ действующим для дальнейшей аутентификации.

Любое программное обеспечение для аутентификации, которое поддерживает алгоритм одноразового пароля на основе времени (TOTP), может использоваться в качестве приложения проверки подлинности. Например, Google Authenticator. Чтобы сгенерировать код безопасности, вы должны синхронизировать время, установленное в приложении проверки подлинности, со временем, установленным для Сервера администрирования.

Приложение проверки подлинности генерирует секретный код следующим образом:

1. Сервер администрирования генерирует специальный секретный ключ и QR-код.
2. Вы передаете сгенерированный секретный ключ или QR-код приложению проверки подлинности.
3. Приложение проверки подлинности генерирует одноразовый код безопасности, который вы передаете в окно аутентификации Сервера администрирования.

Рекомендуется установить приложение проверки подлинности на несколько мобильных устройств. Сохраните секретный ключ (или QR-код) и храните его в надежном месте. Это поможет вам восстановить доступ к Kaspersky Security Center 14.2 Web Console в случае потери доступа к мобильному устройству.

Чтобы обезопасить использование Kaspersky Security Center, вы можете включить двухэтапную проверку для своей учетной записи и включить двухэтапную проверку для всех пользователей.

Вы можете исключить (на стр. 1001) учетные записи из двухэтапной проверки. Это может быть необходимо для служебных учетных записей, которые не могут получить защитный код для аутентификации.

Двухэтапная проверка работает в соответствии со следующими правилами:

- Только пользователь с правом Изменение списков управления доступом объектов (см. стр. 771) функциональной области **Общий функционал**: **Права пользователей**, может включать двухэтапную проверку для всех пользователей.
- Только пользователь, включивший двухэтапную проверку для своей учетной записи, может включить двухэтапную проверку для всех пользователей.
- Только пользователь, включивший двухэтапную проверку для своей учетной записи, может исключить другие учетные записи пользователей из списка двухэтапной проверки, включенной для всех пользователей.
- Пользователь может включить двухэтапную проверку только для своей учетной записи.
- Пользователь, у которого есть право Изменение списков управления доступом объектов (см. стр. 771) функциональной области **Общий функционал**: **Права пользователей** и, который авторизован в Kaspersky Security Center 14.2 Web Console с помощью двухэтапной проверки, может выключать двухэтапную проверку: для любого другого пользователя, только если двухэтапная проверка для всех

пользователей выключена; для пользователя, исключенного из списка двухэтапной проверки включенной для всех пользователей.

- Любой пользователь, выполнивший вход в Kaspersky Security Center 14.2 Web Console с помощью двухэтапной проверки, может повторно получить секретный ключ.
- Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, с которым вы сейчас работаете. Если вы включите этот параметр на Сервере администрирования, вы также включаете этот параметр для учетных записей пользователей его виртуальных Серверов администрирования (см. стр. 169) и не включаете двухэтапную проверку для учетных записей пользователей подчиненных Серверов администрирования.

Если для учетной записи на Сервере администрирования Kaspersky Security Center версии 13 или выше включена двухэтапная проверка, то пользователь не сможет войти в программу Kaspersky Security Center Web Console версий 12, 12.1 или 12.2.

## См. также:

Сценарий:Настройка двухэтапной проверки для всех пользователей .....995

Исключение учетных записей из двухэтапной проверки .....1001

## Включение двухэтапной проверки для вашей учетной записи

Вы можете включить двухэтапную проверку только для своей учетной записи.

Перед тем как включить двухэтапную проверку для своей учетной записи, убедитесь, что на вашем мобильном устройстве установлено приложение проверки подлинности. Убедитесь, что время, установленное в приложении проверки подлинности, синхронизировано со временем устройства, на котором установлен Сервер администрирования.

► *Чтобы включить двухэтапную проверку для учетной записи пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли → Пользователи**.
2. Нажмите на имя вашей учетной записи.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Защита учетной записи**:
   a. Выберите параметр **Запрашивать только имя пользователя, пароль и код безопасности (двухэтапная проверка)**.
   b. В открывшемся окне двухэтапной проверки введите секретный ключ в приложении проверки подлинности или отсканируйте QR-код и получите одноразовый код безопасности.

      Вы можете указать секретный ключ в приложении проверки подлинности вручную или отсканировать QR-код своим мобильным устройством.
   c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением проверки подлинности и нажмите на кнопку **Проверить и применить**.

5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи включена.

### См. также:



## Включение двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для всех пользователей, программа откроет окно включения двухэтапной проверки для вашей учетной записи (на стр. 999).

► *Чтобы включить двухэтапную проверку для всех пользователей:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Дополнительные настройки безопасности** окна свойств **включите двухэтапную проверку для всех пользователей**.

Двухэтапная проверка для всех пользователей включена. Пользователям Сервера администрирования, включая пользователей, которые были добавлены после включения двухэтапной проверки для всех пользователей, необходимо настроить двухэтапную проверку для своих учетных записей, за исключением пользователей, учетные записи которых исключены (см. стр. 1001) из двухэтапной проверки.

### См. также:



## Выключение двухэтапной проверки для учетной записи пользователя

Вы можете выключить двухэтапную проверку для своей учетной записи, а также для учетной записи любого другого пользователя.

Вы можете выключить двухэтапную проверку для других учетных записей пользователей, если у вашей учетной записи есть право Изменение списков управления доступом объектов (см. стр. 771) в области **Общий функционал**: **Права пользователей**.

► *Чтобы выключить двухэтапную проверку для учетной записи пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите выключить двухэтапную проверку. Это может быть ваша собственная учетная запись или учетная запись любого другого пользователя.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Защита учетной записи** выберите параметр **Запрашивать только имя пользователя и пароль** если вы хотите выключить двухэтапную проверку для учетной записи пользователя.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи выключена.

## См. также:

Сценарий:Настройка двухэтапной проверки для всех пользователей .....995

## Выключение двухэтапной проверки для всех пользователей

Вы можете выключить двухэтапную проверку для всех пользователей, если двухэтапная проверка включена для вашей учетной записи и у вашей учетной записи есть право Изменение списков ACL объекта (см. стр. 771) в разделе **Общий функционал**: **Права пользователей**. Если двухэтапная проверка не включена для вашей учетной записи, вы должны включить двухэтапную проверку для своей учетной (см. стр. 999) записи, прежде чем выключить ее для всех пользователей.

► *Чтобы выключить двухэтапную проверку для всех пользователей:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Дополнительные настройки безопасности** окна свойств выключите переключатель **двухэтапной проверки для всех пользователей**.
3. Введите учетные данные своей учетной записи в окне аутентификации.

Двухэтапная проверка для всех пользователей выключена.

## См. также:

Сценарий:Настройка двухэтапной проверки для всех пользователей .....995

Включение двухэтапной проверки для вашей учетной записи .....999

## Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетные записи пользователей из двухэтапной проверки, если у вас есть право Изменение списков ACL объекта (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей**.

Если учетная запись пользователя исключена из списка двухэтапной проверки для всех пользователей, этому пользователю не нужно использовать двухэтапную проверку.

Исключение учетных записей из двухэтапной проверки может быть необходимо для служебных учетных записей, которые не могут передать код безопасности во время аутентификации.

► *Если вы хотите исключить некоторые учетные записи пользователей из двухэтапной проверки:*

1. Сначала необходимо выполнить опрос Active Directory (см. стр. 329), чтобы обновить список пользователей Сервера администрирования, если вы хотите исключить учетные записи Active Directory.
2. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На закладке **Дополнительные настройки безопасности** окна свойств в таблице исключений для двухэтапной проверки нажмите на кнопку **Добавить**.
4. В открывшемся окне:
   a. Выберите учетную запись пользователя, которую вы хотите исключить.
   b. Нажмите на кнопку **ОК**.

Выбранные учетные записи пользователей исключены из двухэтапной проверки.

### См. также:

Сценарий:Настройка двухэтапной проверки для всех пользователей .....995
О двухэтапной проверке .....997

## Генерация нового секретного ключа

Вы можете сгенерировать новый секретный ключ для двухэтапной проверки своей учетной записи, только если вы авторизованы с помощью двухэтапной проверки.

► *Чтобы сгенерировать новый секретный ключ для учетной записи пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись пользователя, для которой вы хотите сгенерировать новый секретный ключ для двухэтапной проверки.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Защита учетной записи** перейдите по ссылке **Сгенерировать новый секретный ключ**.
5. В открывшемся окне двухэтапной проверки укажите новый ключ безопасности, сгенерированный приложением проверки подлинности.
6. Нажмите на кнопку **Проверить и применить**.

Новый секретный ключ для пользователя создан.

Если вы потеряете свое мобильное устройство, можно установить приложение проверки подлинности на другое мобильное устройство и сгенерировать новый секретный ключ для восстановления доступа к Kaspersky Security Center 14.2 Web Console.

### Изменение имени издателя кода безопасности

У вас может быть несколько идентификаторов (также их называют издателями) для разных Серверов администрирования. Вы можете изменить имя издателя кода безопасности, например, если Сервер администрирования уже использует аналогичное имя издателя кода безопасности для другого Сервера администрирования. По умолчанию имя издателя кода безопасности совпадает с именем Сервера администрирования.

После изменения имени издателя кода безопасности необходимо повторно выпустить новый секретный ключ и передать его приложению проверки подлинности.

► *Чтобы указать новое имя издателя кода безопасности:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
3. На закладке **Защита учетной записи**, перейдите по ссылке **Редактировать**.

   Откроется раздел **Изменить издателя кода безопасности**.
4. Укажите новое имя издателя кода безопасности.
5. Нажмите на кнопку **ОК**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

См. также:

Сценарий:Настройка двухэтапной проверки для всех пользователей .....995

## Резервное копирование и восстановление данных Сервера администрирования

Резервное копирование данных позволяет переносить Сервер администрирования с одного устройства на другое без потерь информации. С помощью резервного копирования вы можете восстанавливать данные при переносе информационной базы Сервера администрирования на другое устройство или при переходе на более позднюю версию Kaspersky Security Center.

Обратите внимание, что резервные копии установленных плагинов управления не сохраняются. После восстановления данных Сервера администрирования из резервной копии необходимо загрузить и переустановить плагины управляемых программ.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных (см. стр. 693) через Консоль администрирования.

- Запустить утилиту klbackup (см. стр. 693) на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы.

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

## Создание задачи резервного копирования данных

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки. Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В окне мастера **Новая задача** выберите тип задачи **Резервное копирование данных Сервера администрирования**.
4. Следуйте дальнейшим шагам мастера.

Задачу **Резервное копирование данных Сервера администрирования** можно создать только в одном экземпляре. Если задача резервного копирования данных Сервера администрирования уже создана для Сервера администрирования, то она не отображается в окне выбора типа задачи мастера создания задачи.

## Перенос Сервера администрирования на другое устройство

Если вам нужно использовать Сервер администрирования на новом устройстве, вы можете перенести его одним из следующих способов:

- Переместить Сервер администрирования и сервер баз данных на новое устройство.
- Оставить сервер баз данных на старом устройстве и перенести на новое устройство только Сервер администрирования.

*Чтобы перенести Сервер администрирования и сервер баз данных на новое устройство:*

1. На предыдущем устройстве создайте резервную копию данных Сервера администрирования.

   Для этого запустите задачу резервного копирования данных (см. стр. 1004) с помощью Kaspersky Security Center 14.2 Web Console или запустите утилиту klbackup (см. стр. 693).

   > Если вы используете SQL Server в качестве СУБД для Сервера администрирования, можно перенести данные с SQL Server на MySQL или MariaDB. Чтобы создать резервную копию данных, запустите утилиту klbackup в интерактивном режиме (см. стр. 693). Включите параметр **Перенос данных в формате MySQL/MariaDB** в окне **Параметры резервного копирования** мастера выполнения резервного копирования и восстановления данных. Kaspersky Security Center создаст резервную копию данных, совместимую с MySQL и MariaDB. После этого вы можете восстановить данные из резервной копии в MySQL или MariaDB.
   > Также можно включить параметр **Перенос в формат Azure**, если вы хотите перенести данные из SQL Server в СУБД Azure SQL (см. стр. ).

2. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям (см. стр. 945) для Сервера администрирования, Kaspersky Security Center 14.2 Web Console и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования доступны (см. стр. 946).
3. На новом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования (см. стр. 164).

   При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.
4. Запустите выборочную установку Сервера администрирования (см. стр. 243) на новом устройстве.
5. Установите компоненты Сервера администрирования в ту же папку (см. стр. 245), где Сервер администрирования установлен на предыдущем устройстве. Нажмите на кнопку **Обзор**, чтобы указать путь к файлу.

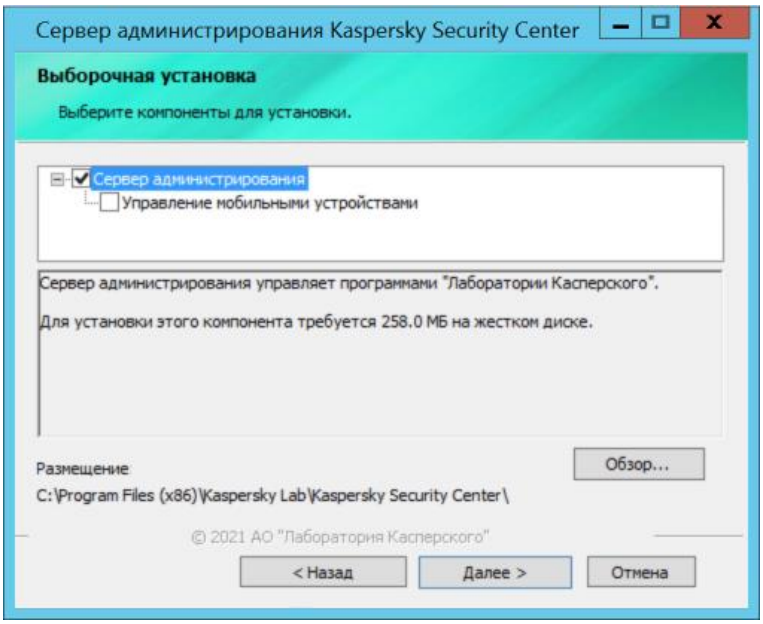



Figure 13. Окно **Выборочная установка**

6. Настройте параметры подключения к серверу базы данных (см. стр. 247).

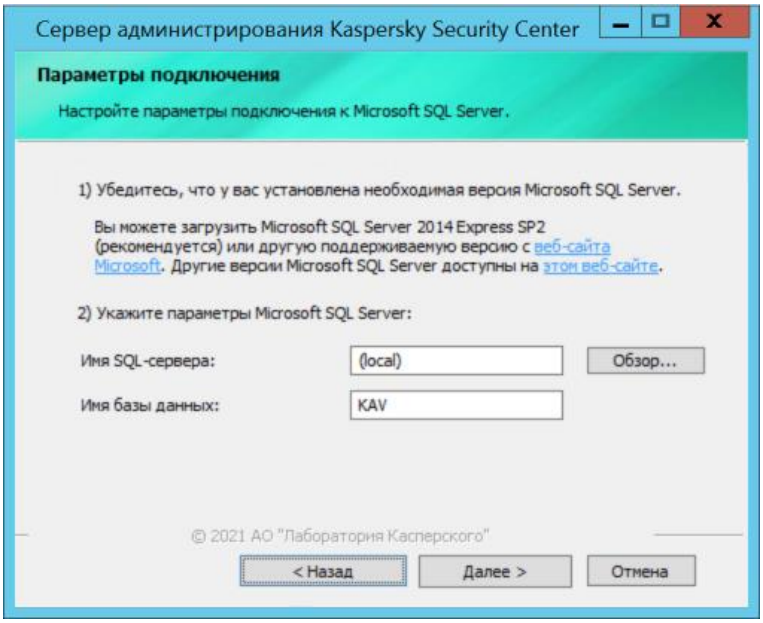



Figure 14. Окно **Параметры подключения**

В зависимости от того, где нужно разместить сервер базы данных, выполните одно из следующих действий:

- Переместите сервер базы данных на новое устройство.
- Оставьте сервер базы данных на предыдущем устройстве.

7. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup (см. стр. 693).

Если вы используете SQL Server в качестве СУБД на предыдущем и новом устройствах, обратите внимание, что версия SQL Server, установленная на новом устройстве, должна быть такой же или выше, чем версия SQL Server, установленная на предыдущем устройстве. Иначе вы не сможете восстановить данные Сервера администрирования на новом устройстве.

8. Откройте Kaspersky Security Center 14.2 Web Console и подключитесь к Серверу администрирования (см. стр. 970).
9. Убедитесь, что все клиентские устройства подключены к Серверу администрирования.
10. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

Также можно использовать Консоль администрирования (см. стр. 697) для переноса Сервера администрирования и сервера баз данных на другое устройство.

kaspersky

### См. также:



# Первоначальная настройка Kaspersky Security Center 14.2 Web Console

В этом разделе описаны шаги, которые необходимо выполнить после установки Kaspersky Security Center 14.2 Web Console для первоначальной настройки.

### В этом разделе



## Мастер первоначальной настройки (Kaspersky Security Center 14.2 Web Console)

В этом разделе представлена информация о работе мастера первоначальной настройки Сервера администрирования.

Мастеру требуется доступ в интернет. Если Сервер администрирования не имеет доступа в интернет, рекомендуется выполнять все шаги мастера вручную через интерфейс Kaspersky Security Center 14.2 Web Console.

Программа Kaspersky Security Center позволяет настроить минимальный набор параметров, необходимых для построения централизованной системы управления, обеспечивающей защиту сети от угроз безопасности. Эта настройка выполняется в мастере первоначальной настройки. В процессе работы мастера вы можете внести в программу следующие изменения:

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить взаимодействие с Kaspersky Security Network (KSN). При разрешении использования KSN мастер включает службу прокси-сервера KSN, которая обеспечивает взаимодействие между KSN и устройствами.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger).

- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вредоносного ПО, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

  Мастер первоначальной настройки создает политики только для программ, для которых еще нет созданных политик в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

Программа автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

► *Чтобы запустить мастер первоначальной настройки вручную:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем главного Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Общие**.
3. Перейдите по ссылке **Запустить мастер первоначальной настройки**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**.

kaspersky

## См. также:



## В этом разделе



## Шаг 1. Указание параметров подключения к интернету

Укажите параметры доступа Сервера администрирования к интернету. Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых программ "Лаборатории Касперского".

Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.

- **Номер порта**

  Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.

- **Не использовать прокси-сервер для локальных адресов**

  При подключении к устройствам в локальной сети не будет использоваться прокси-сервер.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

Поля ввода доступны, если установлен флажок **Использовать прокси-сервер**.

- **Имя пользователя**

  Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

- **Пароль**

  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Вы можете настроить доступ в интернет (см. стр. 982) позднее без запуска мастера первоначальной настройки.

## Шаг 2. Загрузка требуемых обновлений

Необходимые обновления загружаются с серверов "Лаборатории Касперского" автоматически.

## Шаг 3. Выбор активов для защиты

Выберите области защиты и операционные системы, которые используются в вашей сети. При выборе этих параметров вы указываете фильтры для плагинов управления программами и дистрибутивов на серверах "Лаборатории Касперского", которые вы можете загрузить для установки на клиентские устройства в вашей сети. Выберите следующие параметры:

- **Области**

  Вы можете выбрать одну из следующих областей защиты:

  - **Рабочие станции** Выберите этот параметр, если вы хотите защитить рабочие станции в вашей сети. По умолчанию выбран параметр Рабочая станция.
  - **Файловые серверы и системы хранения данных**. Выберите этот параметр, если вы хотите защитить файловые серверы в вашей сети.
  - **Виртуальные среды**. Выберите этот параметр, если вы хотите защитить виртуальные машины в вашей сети.
  - **Банкоматы и POS-системы**. Выберите этот параметр, если вы хотите защитить встроенные системы с операционной системой Windows, например банкоматы (ATM).
  - **Промышленные сети**. Выберите этот параметр, если вы хотите контролировать данные безопасности в промышленной сети и с конечных устройств сети, защищенных программами "Лаборатории Касперского".
  - **Промышленные конечные точки**. Выберите этот параметр, если вы хотите защитить отдельные узлы промышленной сети.

- **Операционные системы**

  Вы можете выбрать одну из следующих платформ:

  - Microsoft Windows;
  - macOS;
  - Android;

- Linux;
- Другое.

Дополнительные сведения о поддерживаемых версиях операционных систем см. в разделе Аппаратные и программные требования Kaspersky Security Center 14.2 Web Console (см. стр. 945).

Можно выбрать инсталляционные пакеты программ "Лаборатории Касперского" (см. стр. 1040) из списка доступных инсталляционных пакетов позднее без запуска мастера первоначальной настройки. Для упрощения поиска необходимых инсталляционных пакетов вы можете фильтровать список доступных инсталляционных пакетов различным критериям.

## Шаг 4. Выбор шифрования

Окно **Шифрование** отображается, только если в качестве области защиты выбран вариант **Рабочие станции**.

Kaspersky Endpoint Security для Windows включает инструменты шифрования информации, хранящейся на клиентских устройствах в операционной системой Windows. Эти инструменты шифрования имеют расширенный стандарт шифрования (AES), реализованный с длиной ключа 256 бит или 56 бит.

Загрузка и использование дистрибутива с длиной ключа 256 бит должна выполняться в соответствии с действующими законами и правилами. Чтобы загрузить дистрибутив Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

В окне **Шифрование** выберите один из следующих типов шифрования:

- Упрощенное шифрование. Для этого типа шифрования используется 56-разрядный ключ.
- Стойкое шифрование. Для этого типа шифрования используется 256-разрядный ключ.

Вы можете выбрать дистрибутив (см. стр. 1040) для Kaspersky Endpoint Security для Windows с необходимым типом шифрования позднее без запуска мастера первоначальной настройки.

## Шаг 5. Настройка установки плагинов для управляемых программ

Выберите плагины для управляемых программ для установки. Отображается список плагинов, расположенных на серверах "Лаборатории Касперского". Список отфильтрован в соответствии с параметрами, выбранными на предыдущем шаге мастера. По умолчанию в полный список включены плагины всех языков. Чтобы отображался только плагин на выбранном языке, используйте фильтр. Список плагинов включает в себя следующие графы:

- **Область защиты**
- **Тип**
- **Имя**

Выбраны подключаемые модули в зависимости от областей защиты и платформ, выбранных на предыдущем шаге.

- **Версия**

В список включены плагины всех версий, размещенных на серверах "Лаборатории Касперского". По умолчанию выбраны плагины последних версий.

- **Последняя версия**
- **Операционная система**
- **Язык**

По умолчанию язык локализации плагина зависит от языка Kaspersky Security Center, который вы выбрали при установке. Другие языки можно выбрать в раскрывающемся списке **Отображать язык Консоли администрирования**.

После выбора подключаемых модулей нажмите на кнопку **Далее**, чтобы начать установку.

Вы можете установить плагины управления для программ "Лаборатории Касперского" (см. стр. 1037) вручную позднее без запуска мастера первоначальной настройки.

Мастер первоначальной настройки автоматически установит выбранные плагины. Для установки некоторых плагинов вы должны принять условия Лицензионного соглашения. Ознакомьтесь с текстом Лицензионного соглашения, который отображается на экране, установите флажок **Я принимаю условия использования Kaspersky Security Network** и нажмите на кнопку **Установить**. Если вы не согласны с условиями Лицензионного соглашения, плагин не установится.

Когда все выбранные плагины будут установлены, мастер первоначальной настройки автоматически перейдет к следующему шагу.

### См. также:

Список поддерживаемых программ "Лаборатории Касперского" и решений.....69

## Шаг 6. Загрузка дистрибутивов и создание инсталляционных пакетов

Выберите дистрибутив для загрузки.

Для дистрибутивов управляемых программ может потребоваться установка определенной минимальной версии Kaspersky Security Center.

После того, как вы выбрали тип шифрования для Kaspersky Endpoint Security для Windows, отобразится список дистрибутивов для обоих типов шифрования. В списке выбран дистрибутив с выбранным типом шифрования. Вы можете выбрать дистрибутив для любого типа шифрования. Язык дистрибутива соответствует языку Kaspersky Security Center. Если дистрибутив Kaspersky Endpoint Security для Windows для языка Kaspersky Security Center не существует, выбирается дистрибутив на английском языке.

Чтобы завершить загрузку некоторых дистрибутивов вы должны принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вы должны принять положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского". Если вы не принимаете положения и условия, загрузка пакета отменяется.

После того, как вы приняли положения и условия Лицензионного соглашения, а также условия Политики конфиденциальности "Лаборатории Касперского", загрузка дистрибутивов продолжается. В дальнейшем инсталляционные пакеты можно использовать для развертывания программ "Лаборатории Касперского" на клиентских устройствах.

Вы можете загрузить дистрибутивы и создать инсталляционные пакеты (см. стр. 1040) позднее без запуска мастера первоначальной настройки.

## Шаг 7. Настройка Kaspersky Security Network

Настройте параметры передачи информации о работе Kaspersky Security Center в базу знаний Kaspersky Security Network. Выберите один из следующих вариантов:

- **Я принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые программы, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять информацию об их работе Kaspersky Security Network (см. стр. 829). Сотрудничество с Kaspersky Security Network обеспечивает более быстрое обновление баз данных о вирусах и угрозах, что увеличивает скорость реагирования на возникающие угрозы безопасности.

- **Я не принимаю условия использования Kaspersky Security Network**

  Kaspersky Security Center и управляемые программы не будут предоставлять информацию о своей работе Kaspersky Security Network.

  Если вы выбрали этот параметр, использование Kaspersky Security Network будет выключено.

Вы можете настроить доступ к Kaspersky Security Network (KSN) (см. стр. 1229) позднее без запуска мастера первоначальной настройки.

## Шаг 8. Выбор способа активации программы

Выберите один из следующих вариантов активации Kaspersky Security Center:

- Введите ваш код активации

  *Код активации* – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Security Center. Код активации отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

  Чтобы активировать программу с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

  Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- Укажите файл ключа

  *Файл ключа* – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

  Файл ключа отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

  Чтобы активировать программу с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в папке **Лицензии "Лаборатории Касперского"** дерева консоли администрирования.

- Отложите активацию программы

  Программа будет работать в режиме Базовой функциональности, без поддержки Управления мобильными устройствами и Системного администрирования.

Если вы отложили активацию программы, вы можете добавить лицензионный ключ позже в любое время, выбрав **Операции** → **Лицензирование**.

При работе с Kaspersky Security Center, развернутым из платного образа AMI или с использованием ежемесячных счетов за использование SKU, вы не можете указать файл ключа или ввести код активации.

## См. также:

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

## Шаг 9. Указание параметров управления обновлениями программ сторонних программ

Этот шаг не отображается, если у вас нет лицензии на Системное администрирование (см. стр. 353), а задача *Поиск уязвимостей и требуемых обновлений* уже существует.

Для обновлений программ сторонних производителей выберите один из следующих вариантов:

- **Искать требуемые обновления**

  Создается задача *Поиск уязвимостей и требуемых обновлений*.

  По умолчанию этот вариант выбран.

- **Искать и устанавливать требующиеся обновления**

Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

Этот параметр доступен при наличии лицензии на Системное администрирование (см. стр. 353).

Для обновлений Центра обновления Windows выберите один из следующих вариантов:

- **Использовать источники обновлений, заданные в политике домена**
- **Использовать Сервер администрирования в роли WSUS-сервера**

Обновления Центра обновления Windows загружаются на клиентские устройства с Сервера администрирования. Задача *Выполнение синхронизации с Центром обновления Windows* и политика Агента администрирования создаются автоматически, если они не были созданы ранее.

Этот параметр доступен при наличии лицензии на Системное администрирование (см. стр. 353).

Вы можете создать (см. стр. 1111) задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* позднее без запуска мастера первоначальной настройки. Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вы должны создать (см. стр. 1309) задачу Синхронизация обновлений Windows Update и включить параметр *Использовать Сервер администрирования в роли WSUS-сервера* в политике Агента администрирования (см. стр. 750).

### См. также:



## Шаг 10. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

Можно создать необходимые задачи (см. стр. 1111) и политики (см. стр. 1174) позднее без запуска мастера первоначальной настройки.

## Шаг 11. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе программ "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках программ.

Для настройки рассылки оповещений о возникающих событиях программ "Лаборатории Касперского" доступны следующие параметры:

- **Электронная почта**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **Адрес SMTP-сервера**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес
  - Имя устройства в сети Windows (NetBIOS-имя)
  - DNS-имя SMTP-сервера

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. Если вы используете несколько SMTP-серверов, соединение с ними устанавливается через указанный коммуникационный порт. По умолчанию установлен порт 25.

- **Требуется ESMTP-аутентификация**

  Включение поддержки ESMTP-аутентификации. После установки флажка в полях **Имя пользователя** и **Пароль** можно указать параметры ESMTP-аутентификации. По умолчанию флажок снят.

- **Использовать TLS**

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**.

Вы можете настроить уведомления о событии (см. стр. 1450) позднее без запуска мастера первоначальной настройки.

### Шаг 12. Выполнение опроса сети

Сервер администрирования выполняет первоначальный опрос сети. Во время опроса отображается ход его выполнения. После завершения опроса ссылка **Просмотреть обнаруженные устройства** становится доступной. Вы можете перейти по ссылке, чтобы просмотреть устройства сети, обнаруженные Сервером администрирования. Чтобы вернуться в мастер первоначальной настройки, нажмите на кнопку **ESCAPE**.

Вы можете выполнить опрос сети позднее без запуска мастера первоначальной настройки. С помощью Kaspersky Security Center Web Console настройте опрос Windows-доменов (см. стр. 1056), Active Directory (см. стр. 1058), IP-диапазонов (см. стр. 1059) и Ipv6-сетей (см. стр. 1063).

#### См. также:

Сценарий: Обнаружение устройств в сети.....1054

### Шаг 13. Завершение работы мастера первоначальной настройки

На странице завершения работы мастера первоначальной настройки установите флажок **Запустить мастер развертывания защиты на рабочих станциях**, если вы хотите запустить автоматическую установку (см. стр. 1028) антивирусных программ или Агента администрирования на устройствах вашей сети.

Для завершения работы мастера нажмите на кнопку **Готово**.

## Подключение автономных устройств

В этом разделе описано, как подключить автономные устройства к Серверу администрирования (то есть управляемые устройства, находящиеся вне основной сети).

kaspersky

## В этом разделе



## Сценарий: Подключение автономных устройств через шлюз соединения

В этом сценарии описано, как подключить к Серверу администрирования управляемые устройства, находящиеся вне основной сети.

### Предварительные требования

Сценарий имеет следующие предварительные требования:

- В сети вашей организации организована демилитаризованная зона (DMZ).
- Сервер администрирования Kaspersky Security Center развернут в корпоративной сети.

### Этапы

Этот сценарий состоит из следующих этапов:

a. **Выбор клиентского устройства в демилитаризованной зоне**

   Это устройство будет использоваться в качестве шлюза соединения (см. стр. 90). Выбранное устройство должно соответствовать требованиям для шлюзов соединения.

b. **Установка Агента администрирования в роли шлюза соединения**

   Для установки Агента администрирования на выбранное устройство рекомендуем использовать локальную установку (см. стр. 378).

   По умолчанию установочный файл находится по адресу: \\<Имя Сервера>\KLSHARE\PkgInst\NetAgent_<номер версии>

   При установке Агента администрирования в окне мастера установки **Шлюз соединений** выбрать вариант **Использовать в качестве шлюза соединений в демилитаризованной зоне**. Этот режим одновременно активирует роль шлюза соединения и предписывает Агенту администрирования ждать соединений от Сервера администрирования, а не устанавливать соединения с Сервером администрирования.

   Также вы можете установить Агент администрирования на устройство под управлением Linux и настроить Агент администрирования для работы в качестве шлюза соединения (см. стр. 663). Обратите внимание на список ограничений Агента администрирования, работающего на устройствах под управлением Linux (см. стр. 935).

c. **Разрешение соединения на сетевом экране шлюза соединения**

   Чтобы Сервер администрирования мог подключаться к шлюзу соединения в демилитаризованной зоне, разрешите подключения к TCP-порту 13000 во всех сетевых экранах между Сервером администрирования и шлюзом соединения.

Если шлюз соединения не имеет реального IP-адреса в интернете, но вместо этого расположен за Network Address Translation (далее также NAT), настройте правило для пересылки подключений через NAT.

**d. Создание группы администрирования для внешних устройств**

Создайте группу (см. стр. 1124) внутри группы **Управляемые устройства**. Эта новая группа будет содержать внешние управляемые устройства.

**e. Подключение шлюза соединения к Серверу администрирования**

Настроенный вами шлюз соединения ожидает соединения от Сервера администрирования. Однако Сервер администрирования не перечисляет устройство со шлюзом соединения среди управляемых устройств. Это связано с тем, что шлюз соединения не пытался установить соединение с Сервером администрирования. Следовательно, вам потребуется особая процедура, чтобы Сервер администрирования инициировал соединение со шлюзом соединения.

Выполните следующие действия:

Добавьте шлюз соединения в качестве точки распространения (см. стр. 1266).

Переместите шлюз соединения (см. стр. 1126) из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

Шлюз соединения подключен и настроен.

**f. Подключение внешних настольных компьютеров к Серверу администрирования**

Обычно внешние настольные компьютеры не перемещаются внутрь периметра сети. Поэтому вам необходимо настроить их для подключения (см. стр. 1021) к Серверу администрирования через шлюз соединения при установке Агента администрирования.

**g. Настройка обновлений для внешних настольных компьютеров**

Если обновления программ безопасности настроены на загрузку с Сервера администрирования, внешние компьютеры загружают обновления через шлюз соединения, что имеет два недостатка. Это имеет два недостатка:

Это лишний трафик, занимающий пропускную способность интернет-канала компании.

Это не обязательно самый быстрый способ получать обновления. Возможно для внешних компьютеров будет удобнее получать обновления с серверов обновлений "Лаборатории Касперского".

Выполните следующие действия:

Переместите все внешние компьютеры в отдельную группу администрирования, (см. стр. 1126) которую вы создали ранее.

Исключить группу с внешними устройствами из задачи обновления (см. стр. 1257).

Создайте отдельную задачу обновления для группы с внешними устройствами (см. стр. 1257).

**h. Подключение ноутбуков к Серверу администрирования**

Иногда ноутбуки находятся внутри сети, а в другое время – вне сети. Для эффективного управления вам необходимо, чтобы они по-разному подключались к Серверу администрирования в зависимости от своего местоположения. Для эффективного использования трафика им также необходимо получать обновления из разных источников в зависимости от их местоположения.

Вам необходимо настроить правила для автономных пользователей (см. стр. 1024): профили подключения (см. стр. 1022) и описания сетевых расположений (см. стр. 1026). Каждое правило определяет экземпляр Сервера администрирования, к которому должны подключаться ноутбуки в зависимости от их местоположения, и экземпляр Сервера администрирования, с которого они должны получать обновления.

См. также:

Доступ в интернет:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне .....166

## О подключении автономных устройств

Некоторые управляемые устройства, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Некоторые устройства время от времени выходят за пределы периметра сети (например, ноутбуки пользователей, которые посещают региональные филиалы или офис клиента).

Вам по-прежнему необходимо отслеживать и управлять защитой устройств вне офиса – получать актуальную информацию об их статусе защиты и поддерживать программы безопасности на них в актуальном состоянии. Это необходимо, например, потому, что если такое устройство будет скомпрометировано, находясь вдали от основной сети, то оно может стать платформой для распространения угроз, как только подключится к основной сети. Для подключения автономных устройств к Серверу администрирования вы можете использовать два способа:

- Шлюз соединения в демилитаризованной зоне (DMZ).

  См. схему трафика данных: Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование шлюза соединения (см. стр. 129).

- Сервер администрирования в демилитаризованной зоне (DMZ)

  См. схему трафика данных: Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете (см. стр. 132).

### Шлюз соединения в демилитаризованной зоне

Рекомендуемый способ подключения автономных устройств к Серверу администрирования это создание демилитаризованной зоны в сети организации и установка шлюза соединения в демилитаризованной зоне (см. стр. 90). Внешние устройства будут подключаться к шлюзу соединения, а Сервер администрирования внутри сети инициирует подключение к устройствам через шлюз соединения.

По сравнению с другим способ этот является более безопасным:

- Вам не нужно открывать доступ к Серверу администрирования извне.
- Скомпрометированный шлюз соединения не представляет большого риска для безопасности сетевых устройств. Шлюз соединения ничем не управляет и не устанавливает никаких соединений.

Кроме того, шлюз соединения не требует много аппаратных ресурсов.

Однако этот способ имеет более сложный процесс настройки:

- Чтобы устройство выполняло роль шлюза соединения в демилитаризованной зоне, вам необходимо установить Агент администрирования и подключить его к Серверу администрирования особым образом.
- Вы не сможете использовать один и тот же адрес подключения к Серверу администрирования для ситуаций. С внешней стороны периметра вам нужно будет использовать не только другой адрес (адрес шлюза соединения), но и другой режим подключения: через шлюз соединения.
- Вам также необходимо определить разные параметры подключения для ноутбуков в разных месторасположениях.

**Сервер администрирования в демилитаризованной зоне (DMZ)**

Другой способ это установка единого Сервера администрирования в демилитаризованной зоне.

Эта конфигурация менее безопасна, чем конфигурация первого способа. В этом случае для управления внешними ноутбуками Сервер администрирования должен принимать соединения с любого адреса из интернета. Сервер администрирования управляет всеми устройствами во внутренней сети, но из демилитаризованной зоны. Поэтому скомпрометированный Сервер может нанести огромный ущерб, несмотря на низкую вероятность такого события.

Риск значительно снижается, если Сервер администрирования в демилитаризованной зоне не управляет устройствами внутренней сети. Такая конфигурация может использоваться, например, поставщиком услуг для управления устройствами клиентов.

Вы можете использовать этот способ в следующих случаях:

- Если вы знакомы с установкой и настройкой Сервера администрирования и не хотите выполнять другую процедуру по установке и настройке шлюза соединения.
- Если вам нужно управлять большим количеством устройств. Максимальное количество устройств, которыми может управлять Сервер администрирования – 100 000 устройств, шлюз соединения может поддерживать до 10 000 устройств.

Это решение также имеет некоторые сложности:

- Серверу администрирования требуется больше аппаратных ресурсов и еще одна база данных.
- Информация об устройствах будет храниться в двух несвязанных между собой базах данных (для Сервера администрирования внутри сети и другой в демилитаризованной зоне), что усложняет контроль.
- Для управления всеми устройствами Сервер администрирования необходимо объединить в иерархию, что усложняет и контроль и управление. Экземпляр подчиненного Сервера администрирования накладывает ограничения на возможные структуры групп администрирования. Вы должны решить, как и какие задачи и политики распространять на подчиненный Сервер администрирования.
- Настройка внешних устройств для использования Сервера администрирования в демилитаризованной зоне извне и для использования главного Сервера администрирования изнутри не проще, чем настройка подключения через шлюз.
- Высокие риски безопасности. Скомпрометированный Сервер администрирования упрощает взлом управляемых ноутбуков. Если это произойдет, хакерам просто нужно дождаться, пока один из ноутбуков вернется в корпоративную сеть, чтобы продолжить атаку на локальную сеть.

## См. также:

Сервер администрирования и два устройства в демилитаризованной зоне: шлюз соединений и клиентское устройство ..... 144

Доступ в интернет:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне ..... 166

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете ..... 132

Шлюз соединения ..... 90

## Подключение внешних настольных компьютеров к Серверу администрирования

Настольные компьютеры, которые всегда находятся вне основной сети (например, компьютеры в региональных филиалах компании; киоски, банкоматы и терминалы, установленные в различных точках продаж; компьютеры в домашних офисах сотрудников), не могут быть подключены к Серверу администрирования напрямую. Они должны быть подключены к Серверу администрирования через шлюз соединения, установленный в демилитаризованной зоне (DMZ). Такая конфигурация выполняется при установке Агента администрирования на эти устройства.

► *Чтобы подключить внешние настольные компьютеры к Серверу администрирования:*

1. Создание инсталляционного пакета Агента администрирования (см. стр. 1038).
2. Откройте свойства созданного инсталляционного пакета, перейдите в раздел **Дополнительно** и включите параметр **Подключаться к Серверу администрирования через шлюз соединений**.

   Параметр **Подключаться к Серверу администрирования через шлюз соединений** несовместим с параметром " **Использовать Агент администрирования в качестве шлюза соединений в демилитаризованной зоне**. Вы не можете включить оба этих параметра одновременно.

3. Укажите адрес шлюза соединения в поле **Адрес шлюза соединений**.

   Если шлюз соединения расположен за Network Address Translation (NAT) и не имеет собственного общедоступного адреса, настройте правило шлюза NAT для перенаправления соединений с общедоступного адреса на внутренний адрес шлюза соединения.
4. Создайте автономный инсталляционный пакет (см. стр. 1041) на основе созданного инсталляционного пакета.
5. Доставьте автономный инсталляционный пакет на целевые компьютеры в электронном виде или на съемном диске.
6. Установите Агент администрирования из автономного инсталляционного пакета.

К Серверу администрирования подключены внешние настольные компьютеры.

## О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

### Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования добавьте профиль для подключения к Серверу администрирования из интернета (в разделе **Параметры программы → Сеть → Профили подключения → Профили подключения к Серверу администрирования**). В окне создания профиля выключите параметр **Использовать только для получения обновлений** и убедитесь, что выбран параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединений в демилитаризованной зоне (см. стр. 166)), в профиле подключения следует указать адрес шлюза соединений в соответствующем поле.

**Переключение между Серверами администрирования в зависимости от текущей сети**

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования создайте профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения укажите адреса соответствующих Серверов администрирования и включите либо выключите параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

## См. также:

Доступ в интернет:Агент администрирования в качестве шлюза соединений в демилитаризованной зоне .....166

Создание профиля соединения для автономных пользователей .....1022

## Создание профиля соединения для автономных пользователей

Подключение профиля Агента администрирования к Серверу администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► *Чтобы создать профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей:*

1. Если вы хотите создать профиль подключения для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:

a. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.

b. Перейдите по ссылке на текущий путь.

c. В открывшемся окне выберите нужную группу администрирования.

После этого текущий путь меняется.

d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.

2. Если вы хотите создать профиль подключения для определенного управляемого устройства, выполните следующие действия, выполните следующие действия:

a. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

b. Нажмите на имя требуемого управляемого устройства.

c. В открывшемся окне свойств управляемого устройства перейдите на закладку **Программы**.

d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.

3. В открывшемся окне свойств перейдите в раздел **Параметры программы** → **Сеть** → **Профили подключения**.

4. В блоке **Профили подключения к Серверу администрирования** нажмите на кнопку **Добавить**.

По умолчанию список профилей подключения содержит профили <Офлайн-режим> и <Домашний Сервер администрирования>. Профили недоступны для изменения и удаления.

В профиле <Офлайн-режим> не указывается Сервер для подключения. При переходе к этому профилю Агент администрирования не пытается подключиться к какому-либо Серверу, а установленные на клиентских устройствах программы используют политики для автономных пользователей. Профиль <Офлайн-режим> применяется в условиях отключения устройств от сети.

В профиле <Домашний Сервер администрирования> указан Сервер для подключения, который был задан при установке Агента администрирования. Профиль <Домашний Сервер администрирования> применяется в условиях, когда устройство, которое работало в другой сети, вновь подключается к домашнему Серверу администрирования.

5. В открывшемся окне **Новый профиль** настройте параметры профиля подключения:

- **Имя профиля**

  В поле ввода можно просмотреть или изменить имя профиля подключения.

- **Сервер администрирования**

  Адрес Сервера администрирования, к которому должно подключаться клиентское устройство при активации профиля.

- **Порт**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

  Номер порта, по которому будет осуществляться подключение с использованием SSL-протокола.

- **Использовать SSL**

  Если этот параметр включен, подключение будет выполняться через защищенный порт (с использованием SSL-протокола).

По умолчанию параметр включен. Чтобы ваше соединение оставалось безопасным, рекомендуется не выключать этот параметр.

- Выберите параметр **Использовать прокси-сервер**, если вы хотите использовать прокси-сервер для подключения к интернету. Если параметр выбран, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:
  - **Адрес прокси-сервера**

    Адрес прокси-сервера для подключения Kaspersky Security Center к интернету.
  - **Номер порта**

    Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center.
  - **Аутентификация на прокси-сервере**
  - **Имя пользователя**
  - **Пароль**
- **Параметры шлюза соединения**

  Адрес шлюза, через который устанавливается соединение клиентских устройств с Сервером администрирования.
- **Включить автономный режим**
- **Использовать только для получения обновлений**

  Если этот параметр включен, профиль будет использоваться только при загрузке обновлений программами, установленными на клиентском устройстве. Для остальных операций подключение к Серверу администрирования будет выполняться с исходными параметрами подключения, заданными при установке Агента администрирования.

  По умолчанию параметр включен.
- **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**

В результате будет создан профиль подключения Агента администрирования к Серверу администрирования для автономных пользователей. При подключении Агента администрирования к Серверу через этот профиль программы, установленные на клиентском устройстве, будут использовать политики для устройств, находящиеся в автономном режиме, или политики для автономных пользователей.

## См. также:

О профилях соединения для автономных пользователей .....1021

## О переключении Агента администрирования на другой Сервер администрирования

В Kaspersky Security Center предусмотрена возможность переключения Агента администрирования клиентского устройства на другие Серверы администрирования при изменении следующих характеристик сети:

- **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.

- **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
- **Условие для DNS-домена** – изменение DNS-суффикса подсети.
- **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
- **Условие для адресов WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для разрешимости имен** – NetBIOS-имя клиентского устройства или DNS-имя было изменено.
- **Условие для подсети** – изменение адреса и маски подсети.
- **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
- **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

Эта функция поддерживается только для Агентов администрирования, установленных на устройствах под управлением Windows или macOS (см. стр. 69).

Исходные параметры подключения Агента администрирования к Серверу задаются при установке Агента администрирования. В дальнейшем, если сформированы правила переключения Агента администрирования на другие Серверы администрирования, Агент реагирует на изменение характеристик сети следующим образом:

- Если характеристики сети соответствуют одному из сформированных правил, Агент администрирования подключается к указанному в этом правиле Серверу администрирования. Если это задано правилом, установленные на клиентских устройствах программы переходят на политики для автономных пользователей.
- Если ни одно из правил не выполняется, Агент администрирования возвращается к исходным параметрам подключения к Серверу администрирования, заданным при установке. Установленные на клиентских устройствах программы возвращаются к активным политикам.
- Если Сервер администрирования недоступен, Агент администрирования использует политики для автономных пользователей.

Агент администрирования переключается на политику для автономных пользователей, только если параметр **Включить автономный режим, когда Сервер администрирования недоступен** (см. стр. 1022) включен в параметрах политики Агента администрирования.

Параметры подключения Агента администрирования к Серверу администрирования сохраняются в профиле подключения. В профиле подключения вы можете создавать правила перехода клиентских устройств на политики для автономных пользователей, а также настраивать профиль таким образом, чтобы он использовался только для загрузки обновлений.

См. также:

Создание правила переключения Агента администрирования по сетевому местоположению.....1026

## Создание правила переключения Агента администрирования по сетевому местоположению

Переключение Агента администрирования доступно только для устройств под управлением операционной системы Windows и macOS.

► *Чтобы создать правило для переключения Агента администрирования с одного Сервера администрирования на другой при изменении характеристик сети:*

1. Если вы хотите создать правило для группы управляемых устройств, откройте политику Агента администрирования этой группы. Для этого выполните следующие:
   a. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
   b. Перейдите по ссылке на текущий путь.
   c. В открывшемся окне выберите нужную группу администрирования.

      После этого текущий путь меняется.
   d. Добавьте политику Агента администрирования для группы управляемых устройств. Если вы уже создали ее, нажмите на название политики Агента администрирования, чтобы открыть свойства политики.
2. Если вы хотите создать правило для определенного управляемого устройства, сделайте следующее:
   a. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
   b. Нажмите на имя требуемого управляемого устройства.
   c. В открывшемся окне свойств управляемого устройства перейдите на закладку **Программы**.
   d. Нажмите на название политики Агента администрирования, к которой применяется только выбранное управляемое устройство.
3. В открывшемся окне свойств перейдите в раздел **Параметры программы** → **Сеть** → **Профили подключения**.
4. В блоке **Параметры сетевого местоположения** нажмите на кнопку **Добавить**.
5. В открывшемся окне свойств настройте описание сетевого местоположения и правило переключения. Настройте следующие параметры описания сетевого местоположения:
   - **Описание**

     Имя описания сетевого местоположения не может превышать 255 символов и содержать специальные символы ("*<>?\/:|).
   - **Использовать профиль подключения**

     В раскрывающемся списке можно выбрать профиль подключения Агента администрирования к Серверу администрирования. Профиль будет использоваться при выполнении условий описания сетевого местоположения. Профиль подключения содержит параметры подключения Агента администрирования к Серверу администрирования и определяет переход клиентских устройств на

политики для автономных пользователей. Профиль используется только для загрузки обновлений.

- **Описание активно**

6. Выберите условия для правила переключения Агента администрирования:
   - **Условие для адреса DHCP-сервера** – изменение IP-адреса DHCP-сервера (Dynamic Host Configuration Protocol) в сети.
   - **Условие для адреса шлюза соединения по умолчанию** – изменение основного шлюза сети.
   - **Условие для DNS-домена** – изменение DNS-суффикса подсети.
   - **Условие для адресов DNS-сервера** – изменение IP-адреса DNS-сервера в сети.
   - **Условие для адресов WINS-сервера** – изменение IP-адреса WINS-сервера в сети. Этот параметр доступен только для устройств с операционными системами Windows.
   - **Условие для разрешимости имен** – NetBIOS-имя клиентского устройства или DNS-имя было изменено.
   - **Условие для подсети** – изменение адреса и маски подсети.
   - **Условие для доступности Windows-домена** – изменение статуса Windows-домена, к которому подключено клиентское устройство. Этот параметр доступен только для устройств с операционными системами Windows.
   - **Условие для доступности адреса SSL-соединения** – клиентское устройство может или не может (в зависимости от выбранного вами параметра) установить SSL-соединение с Сервером (имя:порт). Для каждого Сервера вы можете дополнительно указать SSL-сертификат. В этом случае Агент администрирования проверяет сертификат Сервера администрирования в дополнение к проверке возможности SSL-соединения. Если сертификаты не совпадают, соединение не устанавливается.

   Условия правила объединяются с использованием логического оператора AND. Чтобы правило переключения по описанию сетевого местоположения сработало, все условия переключения правила должны быть выполнены.

7. В разделе с условиями укажите, когда Агент администрирования нужно переключить на другой Сервер администрирования. Для этого нажмите на кнопку **Добавить** и установите значение условия.

   Параметр **Соответствует хотя бы одному значению списка** включен по умолчанию. Можно выключить этот параметр, если вы хотите, чтобы условие выполнялось со всеми указанными значениями.

8. Сохраните изменения.

В результате будет создано правило переключения по описанию сетевого местоположения, при выполнении условий которого Агент администрирования будет использовать для подключения к Серверу администрирования указанный в описании профиль подключения.

## См. также:

О переключении Агента администрирования на другой Сервер администрирования .....1024

kaspersky

# Мастер развертывания защиты

Для установки программ "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку программ как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет расположен: **Опрос сети и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка программы**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 387) и настройте Агент администрирования.

## См. также:



## В этом разделе



# Запуск мастера развертывания защиты

► *Чтобы запустить мастер развертывания защиты вручную,*

в главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

См. также:

Мастер развертывания защиты ..... 1028
Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 1. Выбор инсталляционного пакета

Выберите инсталляционный пакет программы, которую требуется установить.

Если инсталляционный пакет требуемой программы не содержится в списке, нажмите на кнопку **Добавить** и выберите программу из списка.

См. также:

Мастер развертывания защиты ..... 1028
Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 2. Выбор способа распространения файла ключа или кода активации

Выберите способ распространения файла ключа или кода активации:

- **Не добавлять лицензионный ключ в инсталляционный пакет**

  Если выбран этот вариант, ключ будет автоматически распространяться на те устройства, для которых он подходит:

  - если в свойствах ключа настроено автоматическое распространение (см. стр. 395);
  - если создана задача **Добавление ключа**.

- **Добавить лицензионный ключ в инсталляционный пакет**

  Ключ распространяется на устройства вместе с инсталляционным пакетом.

Не рекомендуется распространять ключ таким способом, так как по умолчанию к хранилищу инсталляционных пакетов настроен общий доступ на чтение.

Если инсталляционный пакет уже содержит файл ключа или код активации, это окно отображается, но оно содержит только свойства лицензионного ключа.

См. также:

Мастер развертывания защиты ..... 1028
Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 3. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет программы, отличной от Агента администрирования, необходимо также установить Агент администрирования для подключения программы к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

## Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить программу:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки программы будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

### См. также:

Мастер развертывания защиты ..... 1028

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 5. Задание параметров задачи удаленной установки

На странице **Параметры задачи удаленной установки** настройте параметры удаленной установки программы.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки программы:

- **С помощью Агента администрирования**

  Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

  По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если этот параметр включен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот

вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

Если включен параметр **С помощью Агента администрирования**, файлы будут доставлены средствами операционной системы только в случае невозможности использования средств Агента администрирования.

По умолчанию параметр включен для задач удаленной установки, созданных на виртуальном Сервере администрирования.

- **Средствами операционной системы с помощью Сервера администрирования**

  Если этот параметр включен, доставка файлов на клиентские устройства будет осуществляться средствами операционной системы клиентских устройств с помощью Сервера администрирования. Этот параметр можно включить, если на клиентском устройстве не установлен Агент администрирования, но клиентское устройство находится в той же сети, что и Сервер администрирования.

  По умолчанию параметр включен.

Настройте дополнительные параметры:

- **Не устанавливать программу, если она уже установлена**

  Если этот параметр включен, выбранная программа не устанавливается заново, если она уже установлена на клиентском устройстве.

  Если этот параметр выключен, программа будет установлена в любом случае.

  По умолчанию параметр включен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

## Шаг 6. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки программы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

    После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

### См. также:

Мастер развертывания защиты.....1028

Сценарий: Развертывание программ "Лаборатории Касперского".....1035

## Шаг 7. Удаление несовместимых программ перед установкой

Этот шаг присутствует, только если программа, которую вы разворачиваете, несовместима с другими программами.

Выберите этот параметр, если вы хотите, чтобы программа Kaspersky Security Center автоматически удаляла несовместимые программы с программой, которую вы устанавливаете.

Отображается список несовместимых программ.

Если этот параметр не выбран, программа будет установлена только на устройствах, на которых нет несовместимых программ.

### См. также:

Мастер развертывания защиты ..... 1028

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 8. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Переместить нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

### См. также:

Мастер развертывания защиты ..... 1028

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Шаг 9. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (установка без Агента администрирования)**

Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя для установки программы.

Чтобы указать учетную запись пользователя, под которой будет запускаться программа установки, нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите учетные данные учетной записи пользователя.

Вы можете указать несколько учетных записей, если ни одна из них не обладает необходимыми правами на всех устройствах, для которых назначена задача. В этом случае для запуска задачи используются последовательно, сверху вниз, все добавленные учетные записи.

### См. также:


Мастер развертывания защиты ..... 1028

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035


## Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге задача **Удаленная установка** была успешно создана и настроена.

По умолчанию параметр **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, задача **Удаленная установка** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, задача **Удаленная установка** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **ОК**, чтобы завершить последний шаг мастера развертывания защиты.

### См. также:


Мастер развертывания защиты ..... 1028

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

kaspersky

# Развертывание программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console

В этом разделе описано, как развернуть программы "Лаборатории Касперского" на управляемых устройствах в вашей организации с помощью Kaspersky Security Center 14.2 Web Console.

## В этом разделе



# Сценарий: Развертывание программ "Лаборатории Касперского"

В этом сценарии описана процедура развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console. Можно либо воспользоваться мастером первоначальной настройки (см. стр. 1007) и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

a. **Загрузка веб-плагина управления программы**

   Загрузите веб-плагин управления Kaspersky Endpoint Security для Linuxhttps://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint с сайта "Лаборатории Касперского" и добавьте плагин в Kaspersky Security Center 14.2 Web Console (см. стр. 1037).

b. **Загрузка и создание инсталляционного пакета Агента администрирования**

   Загрузите дистрибутив Агента администрирования https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint с сайта "Лаборатории Касперского", а затем создайте инсталляционный пакет Агента администрирования (см. стр. 1044).

   Вы можете использовать загруженный инсталляционный пакет для локальной установки Агента администрирования. Для этого следуйте инструкциям, приведенным в документации Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.2.0/ru-RU/194971.htm.

c. **Загрузка и создание инсталляционного пакета для Kaspersky Endpoint Security для Linux**

Загрузите дистрибутив Kaspersky Endpoint Security для Linux https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint с сайта "Лаборатории Касперского" и создайте инсталляционный пакет Kaspersky Endpoint Security для Linux (см. стр. 1044).

d. **Создание автономного инсталляционного пакета (если требуется)**

Если вы не можете установить программы "Лаборатории Касперского" с помощью Kaspersky Security Center на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты (см. стр. 1041) для программ. Если вы используете автономные пакеты для установки программ "Лаборатории Касперского" пропустите пункты 5 и 6 этого сценария.

e. **Создание, настройка и запуск задачи удаленной установки**

Этот шаг входит в мастер развертывания защиты. Если вы не запускали мастер развертывания защиты, вам необходимо создать (см. стр. 1111) и настроить эту задачу вручную.

Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одной программы в этих задачах.

Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

> Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 387) и настройте Агент администрирования.

f. **Создание и настройка задач**

Задача *Установка обновлений* Kaspersky Endpoint Security для Linux должна быть настроена.

Этот шаг входит в мастер первоначальной настройки: задача создается и настраивается автоматически, с параметрами по умолчанию. Если вы не запускали мастер первоначальной настройки, вам необходимо создать (см. стр. 1111) и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи (см. стр. 1112) соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

g. **Создание политик**

Создайте политику Kaspersky Endpoint Security для Linux вручную (см. стр. 1174) или с помощью мастера первоначальной настройки. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры (см. стр. 1174) политики в соответствии с вашими требованиями.

h. **Проверка результатов**

Убедитесь (см. стр. 1041), что развертывание завершилось успешно: созданы политики и задачи для каждой программы и эти программы установлены на управляемые устройства.

**Результаты**

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных программ созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.

- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные программы.

## Загрузка плагинов для программ "Лаборатории Касперского"

Для развертывания программ "Лаборатории Касперского", таких как Kaspersky Endpoint Security для Windows, необходимо загрузить плагины управления для этих программ.

► *Чтобы загрузить плагин управления для программы "Лаборатории Касперского":*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Веб-плагины**.
2. В появившемся окне нажмите на кнопку **Добавить**.

   Отобразится список доступных плагинов управления.
3. В списке доступных плагинов выберите имя плагина, который требуется загрузить (например, Kaspersky Endpoint Security 11 для Windows).

   Отобразится страница с описанием плагина.
4. На странице описания плагина нажмите на кнопку **Установить плагин**.
5. После завершения установки нажмите на кнопку **ОК**.

Плагин управления будет загружен в конфигурации по умолчанию и появится в списке плагинов управления.

Вы можете добавлять плагины и обновлять загруженные плагины из файла. Вы можете загрузить плагины управления и веб-плагины управления с сайта Службы технической поддержки "Лаборатории Касперского" https://support.kaspersky.ru/9333.

► *Чтобы загрузить или обновить плагин из файла:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Веб-плагины**.
2. Выполните одно из следующих действий:
   - Нажмите на **Добавить из файла**, чтобы загрузить плагин из файла.
   - Нажмите на **Обновить из файла**, чтобы загрузить обновление для плагина из файла.
3. Укажите файл и подпись файла.
4. Загрузите указанные файлы.

Плагин управления будет загружен в из файла и появится в списке плагинов управления.

### См. также:


Веб-плагин управления ..... 83

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

Плагин управления ..... 82

kaspersky

# Загрузка и создание инсталляционных пакетов для программ "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создать инсталляционные пакеты программ "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского.

► *Чтобы загрузить и создать инсталляционный пакет для программы "Лаборатории Касперского":*

1. Выполните одно из следующих действий:

   - В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для программ "Лаборатории Касперского" в списке экранных уведомлений (см. стр. 1442). Если есть уведомления о новом пакете, вы можете перейти по ссылке рядом с уведомлением к списку доступных инсталляционных пакетов.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На первой странице мастера выберите **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

   Отобразится список инсталляционных пакетов доступных на веб-серверах "Лаборатории Касперского". Список содержит инсталляционные пакеты только тех программ, которые совместимы с текущей версией Kaspersky Security Center.

4. Выберите требуемый инсталляционный пакет, например, Kaspersky Endpoint Security для Windows (11.1.0).

   Откроется окно с информацией об инсталляционном пакете.

   > Вы можете загрузить и использовать инсталляционный пакет, который включает в себя криптографические инструменты, реализующие надежное шифрование, если он соответствует применимым законам и правилам. Чтобы загрузить инсталляционный пакет Kaspersky Endpoint Security для Windows, действительный для нужд вашей организации, обратитесь к законодательству страны, в которой расположены клиентские устройства вашей организации.

5. Ознакомьтесь с информацией и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить дистрибутив** отображается кнопка **Загрузить и создать инсталляционный пакет**.

   Начинается загрузка инсталляционного пакета на Сервер администрирования. Вы можете закрыть окно мастера или перейти к следующему шагу инструкции. Если вы закроете мастер, процесс загрузки продолжится в фоновом режиме.

   Если вы хотите отслеживать процесс загрузки инсталляционного пакета:

   a. В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты** → **В процессе ()**.

b. Следите за ходом операции в графах **Ход загрузки** и **Состояние загрузки** таблицы.

После завершения процесса инсталляционный пакет добавляется в список на закладке **Загружено**. Если процесс загрузки останавливается и статус загрузки меняется на **Принять Лицензионное соглашение**, нажмите на имя инсталляционного пакета и перейдите к следующему шагу инструкции.

> Если размер данных, содержащихся в выбранном дистрибутиве, превышает текущее предельное значение, отображается сообщение об ошибке. Вы можете изменить предельное значение и продолжить создание инсталляционного пакета.

6. Во время процесса загрузки некоторых программ "Лаборатории Касперского" отображается кнопка **Показать Лицензионное соглашение**. Если эта кнопка отображается, выполните следующие действия:

   a. Нажмите на кнопку **Показать Лицензионное соглашение**, чтобы прочитать Лицензионное соглашение (EULA).

   b. Прочитайте появившееся на экране Лицензионное соглашение и нажмите на кнопку **Принять**.

      Загрузка продолжится после того, как вы примете Лицензионное соглашение. Если вы нажмете на кнопку **Отклонить**, загрузка прекратится.

7. После завершения загрузки нажмите на кнопку **Закрыть**.

Выбранный инсталляционный пакет загружен в папку общего доступа Сервера администрирования, во вложенную папку Packages. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

### См. также:

Создание инсталляционного пакета ..... 372

Просмотр экранных уведомлений ..... 1442

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035

## Изменение ограничения на размер пользовательского инсталляционного пакета

Общий размер данных, распакованных при создании пользовательского инсталляционного пакета, ограничен. Ограничение по умолчанию – 1 ГБ.

Если вы попытаетесь загрузить архивный файл, содержащий данные, превышающие текущее ограничение, появится сообщение об ошибке. Возможно, вам придется увеличить это максимальное значение при создании инсталляционных пакетов из больших дистрибутивов.

► *Чтобы изменить максимальное значение для размера пользовательского инсталляционного пакета:*

1. На устройстве Сервера администрирования запустите командную строку под учетной записью, которая использовалась для установки Сервер администрирования (см. стр. 238).
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это <Диск>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. В зависимости от типа установки Сервера администрирования введите одну из следующих команд с правами администратора:

   - Обычная локальная установка:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
     ```

   - Установка отказоустойчивого кластера "Лаборатории Касперского":

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
     --stp klfoc
     ```

   - Установка отказоустойчивого кластера Microsoft:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
     --stp cluster
     ```

   Где <число_байтов> – количество байтов в шестнадцатеричном или десятичном формате.

   Например, если требуемое максимальное значение составляет 2 ГБ, вы можете указать десятичное значение 2147483648 или шестнадцатеричное значение 0x80000000. В этом случае для локальной установки Сервера администрирования вы можете использовать следующую команду:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Ограничение на размер пользовательских данных инсталляционного пакета изменено.

## Загрузка дистрибутивов для программ "Лаборатории Касперского"

В Kaspersky Security Center 14.2 Web Console вы можете загрузить и сохранить дистрибутив для программ "Лаборатории Касперского". Вы можете использовать дистрибутивы для установки программ вручную, без использования Kaspersky Security Center.

► *Чтобы загрузить и сохранить дистрибутив программ "Лаборатории Касперского":*

1. В главном меню перейдите в раздел **Операции** → **Программы "Лаборатории Касперского"** → **Актуальные версии программ**.

   Откроется список доступных дистрибутивов, плагинов и патчей. Kaspersky Security Center отображает только те элементы, которые совместимы с текущей версией программы.

2. В списке нажмите на имя дистрибутива, который вы хотите загрузить.

   Откроется описание дистрибутива.

3. Ознакомьтесь с описанием и нажмите на кнопку **Загрузить и создать инсталляционный пакет**.

   Если дистрибутив не может быть преобразован в инсталляционный пакет, вместо кнопки **Загрузить дистрибутив** отображается кнопка **Загрузить и создать инсталляционный пакет**.

   Начинается загрузка инсталляционного пакета на Сервер администрирования.

Выбранный инсталляционный пакет или дистрибутив загружен в папку общего доступа Сервера администрирования, во вложенную папку **Packages**. После загрузки инсталляционный пакет отображается в списке инсталляционных пакетов.

## Проверка успешности развертывания Kaspersky Endpoint Security

► *Чтобы убедиться, что вы правильно развернули программы "Лаборатории Касперского", например, Kaspersky Endpoint Security:*

1. С помощью Kaspersky Security Center 14.2 Web Console проверьте наличие:
   - политики Kaspersky Endpoint Security и / или других программ безопасности, которые вы используете;
   - задачи для Kaspersky Endpoint Security для Windows: Задача *Быстрый опрос* и *Установка обновлений* (если вы используете Kaspersky Endpoint Security для Windows);
   - задач для других программ безопасности, которые вы используете.
2. Убедитесь, что на управляемых устройствах, для которых была назначена установка:
   - Kaspersky Endpoint Security или другая программа безопасности "Лаборатории Касперского" установлена;
   - параметры Защита от файловых угроз, Защита от веб-угроз и Защита от почтовых угроз соответствуют политике, созданной для этих устройств;
   - можно вручную запустить и остановить службу Kaspersky Endpoint Security;
   - можно вручную запустить и остановить групповые задачи.

### См. также:

Сценарий: Развертывание программ "Лаборатории Касперского" .....1035

## Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки программ на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл (installer.exe), который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center. Вы можете создавать автономные инсталляционные пакеты как для программ "Лаборатории Касперского", так и для программ сторонних производителей для Windows, macOS и Linux. Чтобы создать автономный инсталляционный пакет для программ сторонних производителей, необходимо создать пользовательский инсталляционный пакет (см. стр. 1044).

Убедитесь, что автономный инсталляционный пакет не доступен для неавторизованных лиц.

► *Чтобы создать автономный инсталляционный пакет:*

1. Выполните одно из следующих действий:
   - В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

- В главном окне программы перейдите в раздел **Операции → Хранилища → Инсталляционные пакеты**.

Отобразится список инсталляционных пакетов доступных на Сервере администрирования.

2. В списке инсталляционных пакетов выберите пакет и над списком нажмите на кнопку **Развернуть**.
3. Выберите параметр **С использованием автономного инсталляционного пакета**.

   В результате запускается мастер создания автономного инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На первой странице мастера убедитесь, что включен параметр **Установить Агент администрирования совместно с данной программой**, если требуется установить Агент администрирования совместно с выбранной программой.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

   Если автономный инсталляционный пакет для выбранной программы уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вы должны выбрать одно из следующих действий:

   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии программы, и чтобы также остался автономный инсталляционный пакет для предыдущей версии программы, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.
   - **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
   - **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этой же программы еще раз. Автономный инсталляционный пакет размещается в той же папке.
5. На странице мастера **Перемещение в список управляемых устройств** по умолчанию включен параметр **Не перемещать устройства**. Если вы не хотите перемещать клиентское устройство в какую-либо группу администрирования после установки Агента администрирования, оставьте этот параметр включенным.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.
6. На следующей странице мастера, после завершения процесса создания автономного инсталляционного пакета, нажмите на кнопку **Готово**.

   Мастер создания автономного инсталляционного пакета закрывается.

Автономный инсталляционный пакет создан и помещен во вложенную папку PkgInst общей папки Сервера администрирования (см. стр. 236). Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных инсталляционных пакетов**, расположенную над списком инсталляционных пакетов.

См. также:

Сценарий: Развертывание программ "Лаборатории Касперского" .....1035

## Просмотр списка автономных инсталляционных пакетов

Вы можете просмотреть список автономных инсталляционных пакетов и свойства каждого отдельного инсталляционного пакета.

► *Чтобы просмотреть список автономных инсталляционных пакетов для всех инсталляционных пакетов:*

Над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии программы, включенной в пакет.
- **Название программы**. Имя программы, которая включена в автономный инсталляционный пакет.
- **Версия программы**.
- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Размер**. Размер файла (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Путь**. Полный путь к папке, в которой находится автономный инсталляционный пакет.
- **Веб-адрес**. Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла**. Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

► *Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,*

выберите инсталляционный пакет в списке над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.

- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Загрузить**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

## Создание пользовательского инсталляционного пакета

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любую программу (такую как текстовый редактор) на клиентские устройства, например, с помощью задачи (см. стр. 1108);
- создать автономный инсталляционный пакет (см. стр. 1041).

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет. Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки программы в тихом режиме.

Если у вас есть активный лицензионный ключ для функции Системного администрирования, вы можете преобразовать параметры установки по умолчанию для соответствующего пользовательского инсталляционного пакета и использовать значения, рекомендованные специалистами "Лаборатории Касперского". Параметры автоматически преобразуются при создании пользовательского инсталляционного пакета, только если соответствующий исполняемый файл включен в базу данных программ сторонних производителей "Лаборатории Касперского".

► *Чтобы создать пользовательский инсталляционный пакет:*

1. Выполните одно из следующих действий:
   - В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Отобразится список инсталляционных пакетов доступных на Сервере администрирования.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На первой странице мастера выберите **Создать инсталляционный пакет из файла**.
4. На следующей странице мастера укажите имя пакета и нажмите на кнопку **Обзор**.

   Откроется стандартное окно Windows **Открыть**, в котором можно выбрать файл для создания инсталляционного пакета.

5. Выберите архивный файл, расположенный на доступных дисках.

   Вы можете загрузить архивный файл формата ZIP, CAB, TAR или TAR.GZ. Создать установочный пакет из файла формата SFX (самораспаковывающийся архив) нельзя.

   > Если вы хотите, чтобы параметры были преобразованы во время установки пакета, убедитесь, что установлен флажок **Конвертировать параметры на рекомендуемые значения для программ, распознаваемых Kaspersky Security Center** и нажмите на кнопку **Далее**.

   Начнется загрузка файла на Сервер администрирования Kaspersky Security Center.

   > Если вы включили использование рекомендуемых параметров установки, Kaspersky Security Center 14.2 проверяет, включен ли исполняемый файл в базу данных программ сторонних производителей "Лаборатории Касперского". Если проверка прошла успешно, вы получите уведомление о том, что файл распознан. Параметры сконвертированы и пользовательский инсталляционный пакет создан. Никаких дальнейших действий не требуется. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

6. На следующей странице мастера выберите файл (из списка файлов, которые извлечены из выбранного архивного файла) и укажите параметры командной строки исполняемого файла.

   Вы можете указать параметры командной строки для установки программы из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

7. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования (см. стр. 236). После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя**. Название инсталляционного пакета.
  - **Источник**. Имя поставщика программы.
  - **Программа**. Название программы, упакованной в пользовательский инсталляционные пакет.
  - **Версия**. Версия программы.
  - **Язык**. Язык программы, упакованной в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **Операционная система**. Тип операционной системы, для которой предназначен инсталляционные пакет.
  - **Создано**. Дата создания инсталляционного пакета.
  - **Изменено**. Дата изменения инсталляционного пакета.

- **Тип**. Тип инсталляционного пакета.

- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе программ "Лаборатории Касперского".

Если во время конвертации вы установили рекомендуемые значения параметров для создания пользовательского пакета, могут появиться два дополнительных раздела на закладке **Параметры** в свойствах пользовательского инсталляционного пакета: **Параметры** и **Последовательность установки**.

Разделе **Параметры** содержит следующие свойства, представленные в таблице:

- **Название**. В этом столбце отображается имя, назначенное параметру установки.
- **Тип**. В этом столбце указан тип параметра установки.
- **Значение**. В этом столбце отображается тип данных, определенный параметром установки (логическое значение, путь к файлу, числовое значение, путь или строковое значение).

Раздел **Последовательность установки** содержит таблицу, в которой описаны следующие свойства обновления, включенного в пользовательский инсталляционный пакет:

- **Название**. Название обновления.
- **Описание**. Описание обновления.
- **Источник**. Источник обновления, то есть выпущено ли обновление Microsoft или другим сторонним производителем.
- **Тип**. Тип обновления, то есть предназначено ли обновление для драйвера или программы.
- **Категория**. Категория служб Windows Server Update Services (WSUS), отображаемая для обновлений Microsoft (Критические обновления, Обновления определений, Драйверы, Пакеты дополнительных компонентов, Обновления системы безопасности, Пакеты обновления, Средства, Накопительные пакеты обновления, Обновления или Обновления с предыдущих версий).
- **Уровень важности по MSRC**. Уровень важности обновления, определенный Microsoft Security Response Center (MSRC).
- **Уровень важности**. Уровень важности обновления определен "Лабораторией Касперского".
- **Уровень важности патча (для патчей программ "Лаборатории Касперского")**. Уровень важности патча, если он предназначен для программ "Лаборатории Касперского".
- **Статья**. Идентификатор статьи в Базе знаний с описанием обновления.
- **Бюллетень**. Идентификатор бюллетеня безопасности с описанием обновления.
- **Не назначено к установке**. Отображается, имеет ли обновление статус Не назначено к установке.
- **Назначено к установке**. Отображается, имеет ли обновление статус Назначено к установке.
- **Устанавливается**. Отображается, имеет ли обновление статус Устанавливается.
- **Установлено**. Отображается, имеет ли обновление состояние Установлено.
- **Сбой**. Отображается, имеет ли обновление статус Сбой.
- **Требуется перезагрузка**. Отображается, имеет ли обновление статус Требуется перезагрузка.
- **Зарегистрировано**. Отображается дата и время, когда обновление было зарегистрировано.

- **Устанавливается интерактивно**. Отображается, требуется ли взаимодействие с пользователем во время установки обновления.
- **Отозвано**. Отображается дата и время, когда обновление было отозвано.
- **Статус одобрения обновления**. Отображается, одобрена ли установка обновления.
- **Ревизия**. Отображается номер текущей ревизии обновления.
- **Идентификатор обновления**. Отображается идентификатор обновления.
- **Версия программы**. Отображается номер версии, до которой будет обновлена программа.
- **Заменяемое**. Отображаются другие обновления, которые могут заменить это обновление.
- **Заменяющее**. Отображаются другие обновления, которые можно заменить этим обновлением.
- **Требуется принять условия Лицензионного соглашения**. Отображается, требует ли обновление согласие с условиями Лицензионного соглашения.
- **Поставщик**. Отображается имя поставщика обновлений.
- **Семейство программ**. Отображается имя семейства программ, к которым относится обновление.
- **Программа**. Отображается название программы, которой принадлежит обновление.
- **Язык**. Отображается язык локализации обновления.
- **Не назначено к установке (новая версия)**. Отображается, имеет ли обновление статус Не назначено к установке (новая версия).
- **Требует установки пререквизитов**. Отображается, имеет ли обновление состояние Требует установки пререквизитов.
- **Режим загрузки**. Отображается режим загрузки обновлений.
- **Является патчем**. Отображается, является ли обновление патчем.
- **Не установлено**. Отображается, имеет ли обновление статус Не установлено.

### См. также:


Создание инсталляционного пакета ..... 372

Просмотр экранных уведомлений ..... 1442

Сценарий: Развертывание программ "Лаборатории Касперского" ..... 1035


## Распространение инсталляционных пакетов на подчиненные Серверы администрирования

Kaspersky Security Center позволяет вам создавать инсталляционные пакеты для программ "Лаборатории Касперского" и для программ сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать программы из пакетов. Для оптимизации нагрузки на главном Сервере администрирования вы можете распространять инсталляционные пакеты на подчиненные Серверы администрирования. После этого подчиненные Серверы передают пакеты на клиентские устройства, после чего вы можете выполнять удаленную установку программ на свои клиентские устройства.

► *Чтобы распространить инсталляционные пакеты на подчиненные Серверы администрирования:*

1. Убедитесь что подчиненные Серверы администрирования подключены к главному Серверу администрирования.
2. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.

   Отобразится список задач.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
4. На странице **Новая задача** в раскрывающемся списке **Программа** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространить инсталляционный пакет** и укажите имя задачи.
5. На странице **Область действия задачи** выберите устройства, которым назначена задача, одним из следующих способов:
   - Если вы хотите сформировать задачу для всех подчиненных Серверов определенной группы администрирования, выберите эту группу и запустите создание групповой задачи для этой группы.
   - Если вы хотите создать задачу для определенных подчиненных Серверов администрирования, выберите эти Серверы и создайте для них задачу.
6. На странице **Распространяемые инсталляционные пакеты** выберите инсталляционные пакеты, которые необходимо скопировать на подчиненные Серверы администрирования.
7. Укажите учетную запись для запуска задачи *Распространение инсталляционного пакета* под этой учетной записью. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.
8. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию (см. стр. 1112). Также можно настроить параметры задачи позже в любое время.
9. Нажмите на кнопку **Готово**.

   Задача, созданная для распространения инсталляционных пакетов на подчиненные Серверы администрирования, отображается в списке задач.
10. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи выбранные инсталляционные пакеты скопированы на указанные подчиненные Серверы администрирования.

## Установка программ с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке (см. стр. 383).

## В этом разделе



## Установка программы на выбранные устройства

Этот раздел содержит информацию о том, как удаленно установить программу на устройства в группе администрирования, устройства с определенными IP-адресами или набор управляемых устройств.

► *Чтобы установить программу на выбранные устройства:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка программы**.
4. Выберите один из следующих вариантов:
   - **Назначить задачу группе администрирования**

     В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.
   - **Задать адреса устройств вручную или импортировать из списка**

Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

5. Следуйте далее указаниям мастера.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

6. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки, выбранная программа устанавливается на указанный набор устройств.

## См. также:

Мастер развертывания защиты.....1028

## Установка программы с помощью групповых политик Active Directory

Kaspersky Security Center позволяет устанавливать программы "Лаборатории Касперского" на управляемые устройства с помощью групповых политик Active Directory.

Установка программ с помощью групповых политик Active Directory возможна только из инсталляционных пакетов, в состав которых входит Агент администрирования.

► *Чтобы установить программу с помощью групповых политик Active Directory:*

1. Запустите мастер развертывания защиты (см. стр. 383). Следуйте далее указаниям мастера.
2. На странице **Параметры задачи удаленной установки** (см. стр. 1030) мастера развертывания защиты выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.
3. В окне мастера удаленной установки **Выбор учетных записей для доступа к устройствам** (см. стр. 1033) выберите параметр **Учетная запись требуется (Агент администрирования не используется)**.
4. Добавьте учетную запись с правами администратора на устройство, на котором установлен Kaspersky Security Center, или учетную запись, входящую в доменную группу Владельцы-создатели групповой политики.
5. Предоставьте разрешения выбранной учетной записи:

a. Перейдите в **Панель управления** → **Администрирование** и откройте **Управление групповой политикой**.

b. Нажмите на узел с нужным доменом.

c. Нажмите на раздел **Делегирование**.

d. В раскрывающемся списке **Права доступа** выберите **Связанные объекты GPO**.

e. Нажмите на кнопку **Добавить**.

f. В открывшемся окне **Выбор пользователя, компьютера или группы** выберите необходимую учетную запись.

g. Нажмите на кнопку **ОК** чтобы закрыть окно **Выбор пользователя, компьютера или группы**.

h. В списке **Группы и пользователи** выберите только что добавленную учетную запись и нажмите на **Дополнительно** → **Дополнительно**.

i. В списке **записей разрешений** дважды нажмите на только что добавленную учетную запись.

j. Предоставьте следующие разрешения:

- **создание объектов группы;**
- **удаление объектов группы;**
- **создание объектов контейнера групповой политики;**
- **удаление объектов контейнера групповой политики.**

k. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

6. Задайте другие параметры, следуя инструкциям мастера.
7. Запустите созданную задачу удаленной установки вручную или дождитесь ее запуска по расписанию.

В результате будет запущен следующий механизм удаленной установки:

1. После запуска задачи в каждом домене, которому принадлежат клиентские устройства из набора, будут созданы следующие объекты:
   - Объект групповой политики (Group policy object, GPO) с именем **Kaspersky_AK{GUID}**.
   - Группа безопасности содержит клиентские устройства, на которые распространяется задача. Эта группа безопасности содержит клиентские устройства, на которые распространяется задача. Состав группы безопасности определяет область объект групповой политики (GPO).
2. Kaspersky Security Center устанавливает выбранные программы "Лаборатории Касперского" на клиентские устройства осуществляется непосредственно из сетевой папки общего доступа программы Share. При этом в папке установки Kaspersky Security Center будет создана вложенная вспомогательная папка, содержащая файл с расширением msi для устанавливаемой программы.
3. При добавлении новых устройств в область действия задачи они будут добавлены в группу безопасности после следующего запуска задачи. Если в расписании задачи выбран флажок **Запускать пропущенные задачи**, устройства будут добавлены в группу безопасности сразу.
4. При удалении устройств из области действия задачи их удаление из группы безопасности произойдет при следующем запуске задачи.
5. При удалении задачи из Active Directory будут удалены объект групповой политики (GPO), ссылка на объект групповой политики (GPO) и группа безопасности, связанная с задачей.

Если вы хотите использовать другую схему установки через Active Directory, вы можете настроить параметры

установки вручную. Это может потребоваться, например, в следующих случаях:

- при отсутствии у администратора антивирусной безопасности прав на внесение изменений в Active Directory некоторых доменов;
- при необходимости размещения исходного дистрибутива на отдельном сетевом ресурсе;
- для привязки групповой политики к конкретным подразделениям Active Directory.

Доступны следующие варианты использования другой схемы установки через Active Directory:

- Если установку требуется осуществлять непосредственно из папки общего доступа Kaspersky Security Center, в свойствах групповой политики Active Directory следует указать файл с расширением msi, расположенный во вложенной папке exec в папке инсталляционного пакета нужной программы.
- Если инсталляционный пакет нужно разместить на другом сетевом ресурсе, следует скопировать в него все содержимое папки exec, так как помимо файла с расширением msi в ней содержатся конфигурационные файлы, сформированные при создании инсталляционного пакета. Чтобы лицензионный ключ был установлен вместе с программой, в эту папку следует также скопировать файл ключа.

### Установка программ на подчиненные Серверы администрирования

► *Чтобы установить программу на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи (см. стр. 1111) **Распространение инсталляционного пакета**.
3. Создайте задачу удаленной установки программы (см. стр. 1049) на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка программы на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранная программа устанавливается на подчиненные Серверы администрирования.

## Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете программу на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

► *Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.

2. Нажмите на имя задачи удаленной установки, для которой вы хотите указать параметры, специфичные для Unix.

   Откроется окно свойств задачи.

3. Перейдите в **Параметры программы → Параметры для Unix**.
4. Задайте следующие параметры:
   - **Установить пароль для учетной записи root (только для развертывания через SSH)**
   - **Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)**
5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

### См. также:

Общие параметры задач.....1112

Сценарий: Развертывание программ "Лаборатории Касперского".....1035

Сценарий: Мониторинг и отчеты.....1360

## Замещение программ безопасности сторонних производителей

Для установки программ безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Kaspersky Security Center предоставляет несколько способов удаления программ сторонних производителей.

**Удаление несовместимых программ с помощью программы установки**

Этот параметр доступен только в Консоли администрирования на основе консоли управления Microsoft Management Console.

Метод удаления несовместимых программ поддерживается различными типами установки. Перед установкой программы безопасности несовместимые с ней программы удаляются автоматически, если в окне свойств инсталляционного пакета программы безопасности (раздел **Несовместимые программы**) включен параметр **Удалять несовместимые программы автоматически**.

**Удаление несовместимых программ при настройке удаленной установки программы**

Вы можете включить параметр **Удалять несовместимые программы автоматически** во время настройки удаленной установки программы безопасности. В Консоли администрирования на основе консоли Microsoft Management Console (MMC) этот параметр доступен в мастере удаленной установки. В программе Kaspersky Security Center 14.2 Web Console этот параметр можно найти в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые программы перед установкой программы безопасности на управляемое устройство.

Инструкции:

- Консоль администрирования: Установка программ с помощью мастера удаленной установки (см. стр. 365).

- Kaspersky Security Center 14.2 Web Console: Удаление несовместимых программ перед установкой (см. стр. 1032).

**Удаление несовместимых программ с помощью отдельной задачи**

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы безопасности не может успешно удалить какую-либо из несовместимых программ.

Инструкции для Консоли администрирования: Создание задачи (см. стр. 413)

# Обнаружение устройств в сети

В этом разделе описаны поиск устройств и опрос сети.

Kaspersky Security Center позволяет искать устройства на основании заданных критериев. Вы можете сохранить результаты поиска в текстовый файл.

Функция поиска позволяет находить следующие устройства:

- клиентские устройства в группах администрирования Сервера администрирования Kaspersky Security Center и его подчиненных Серверов;
- нераспределенные устройства под управлением Сервера администрирования Kaspersky Security Center и его подчиненных Серверов.

## В этом разделе



## Сценарий: Обнаружение устройств в сети

Вы должны выполнить поиск устройств перед установкой программ безопасности. Сервер администрирования получает информацию об обнаруженных устройствах и позволяет управлять устройствами с помощью политик. Регулярные опросы сети необходимы для обновления списка устройств, доступных в сети.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

Обнаружение сетевых устройств содержит следующие этапы:

a. **Обнаружение устройств**

Мастер первоначальной настройки выполняет начальное обнаружение устройств (см. стр. 299) и помогает найти сетевые устройства, такие как компьютеры, планшеты и мобильные телефоны. Вы можете также запустить обнаружение устройств вручную (см. стр. 325).

b. **Настройка расписания опросов**

Определите, какой тип опроса (см. стр. 325) вы хотите регулярно использовать. Включите нужные типы опроса и настройте необходимое расписание опроса. Также см. рекомендации по частоте опроса сети.

c. **Задание правил для добавления обнаруженных устройств в группы администрирования (если требуется)**

Новые устройства появляются в сети в результате их обнаружения при опросах сети. Они автоматически попадают в группу **Нераспределенные устройства**. Можно настроить правила перемещения устройств (см. стр. 445), в соответствии с которыми устройства будут распределены в группу **Управляемые устройства**. Можно также настроить правила хранения (см. стр. 333).

Если вы пропустили шаг 3, список новых обнаруженных устройств располагается в группе **Нераспределенные устройства**. Вы можете переместить эти устройства в группу **Управляемые устройства** вручную. Если вы вручную переместили устройства в группу **Управляемые устройства**, вы можете проанализировать информацию о каждом из устройств и решить, требуется ли переместить его в группу администрирования и в какую.

**Результаты**

Завершение сценария дает следующее:

- Сервер администрирования Kaspersky Security Center обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.
- Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

# Обнаружение устройств

В этом разделе описаны типы обнаружения устройств, доступные в Kaspersky Security Center, а также приведена информация об использовании каждого из них.

Во время регулярных опросов сети Сервер администрирования получает информацию о структуре сети и устройствах в сети. Данные записываются в базу данных Сервера администрирования. Сервер администрирования может проводить следующие типы опросов сети:

- **Включить опрос сети Windows**. Сервер администрирования может проводить два типа опросов сети Windows: быстрый и полный. При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. При полном опросе с каждого клиентского устройства запрашивается более подробная информация, например, имя операционной системы, IP-адрес, DNS-имя и NetBIOS-имя. По умолчанию включены быстрый и полный опрос. При опросе сети Windows может не удаться обнаружить устройства, например, если роутером или сетевым экраном закрыты порты UDP 137, UDP 138, TCP 139.
- **Опрос Active Directory**. Сервер администрирования получает информацию о структуре групп Active Directory, а также информацию о DNS-именах устройств, входящих в группы Active Directory. По умолчанию этот тип опроса включен. При использовании Active Directory рекомендуется использовать

опрос Active Directory. В противном случае Сервер администрирования не сможет обнаружить устройства. Если используется Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

- **Опрос IP-диапазона**. Сервер администрирования опрашивает указанные IP-диапазоны с помощью ICMP-пакетов или NBNS-протоколов и получает полную информацию об устройствах, входящих в IP-диапазоны. По умолчанию этот тип опроса выключен. Не рекомендуется использовать этот тип опроса, если вы используете опрос сети Windows и / или опрос Active Directory.
- **Опрос Zeroconf**. Точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). По умолчанию этот тип опроса выключен. Вы можете использовать опрос Zeroconf, если точка распространения работает под управлением Linux.

Если вы настроили и включили правила перемещения устройств (см. стр. 445), новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства**. Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Можно изменить параметры обнаружения устройств для каждого типа. Например, может потребоваться изменить расписание опроса или указать, нужно опрашивать весь лес Active Directory или только определенный домен.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

## См. также:

Сценарий: Обнаружение устройств в сети ..... 324
Основной сценарий установки ..... 92

## В этом разделе



# Опрос сети Windows

### Об опросе сети Windows

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- имя операционной системы;

- IP-адрес;
- DNS-имя;
- NetBIOS-имя.

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

**Просмотр и изменение параметров опроса сети Windows**

► *Чтобы изменить параметры опроса сети Windows:*

1. В главном окне программы перейдите в раздел Обнаружение устройств и развертывание → **Обнаружение устройств** → **Windows-домены**.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Windows-домена.
3. Включите или выключите опрос Windows сети, используя переключатель **Включить опрос сети Windows**.
4. Настройте расписание опроса. По умолчанию быстрый опрос запускается каждые 15 минут, а полный опрос запускается каждые 60 минут.

   Варианты расписания опроса:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.
   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.
   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.
   - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.
   - **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр выключен.

5. Нажмите на кнопку **Сохранить**.

Параметры сохранены и применены ко всем Windows-доменам и рабочим группам.

**Запуск опроса вручную**

► *Чтобы запустить проверку немедленно,*

На кнопку **Начать быстрый опрос** или **Начать полный опрос**.

Когда опрос завершен, вы можете просмотреть список обнаруженных устройств на странице **Windows-домены**, установив флажок рядом с именем домена, а затем нажать на кнопку **Устройства**.

См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Опрос Active Directory

Используйте опрос Active Directory, если вы используете Active Directory; в противном случае рекомендуется использовать другие типы опросов. Если вы используете Active Directory, но отдельные сетевые устройства не являются его членами, эти устройства не удастся обнаружить при опросе Active Directory.

Kaspersky Security Center отправляет запрос к доменному контроллеру и получает структуру устройств Active Directory. Опрос Active Directory осуществляется каждый час.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

**Просмотр и изменение параметров опроса Active Directory**

► *Чтобы просмотреть и изменить параметры опроса Active Directory:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Active Directory**.
2. Нажмите на кнопку **Свойства**.

   В результате откроется окно свойств Active Directory.
3. В окне свойств Active Directory укажите следующие параметры:

   a. С помощью переключателя включите или выключите опрос Active Directory.

b. Настройте расписание опроса.

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

c. Выполните настройку дополнительных параметров и задайте область опроса:

- Домен Active Directory, к которому относится Kaspersky Security Center.
- Лес доменов, к которому относится Kaspersky Security Center.
- Указанный список доменов Active Directory.

Чтобы добавить домен к области опроса, выберите параметр Домен, нажмите на кнопку **Добавить**, укажите адрес доменного контроллера, а также имя и пароль учетной записи для доступа к нему.

4. Нажмите на кнопку **Сохранить**, чтобы указанные параметры вступили в силу.

Указанные параметры будут применяться при опросе Active Directory.

**Запуск опроса вручную**

► *Чтобы запустить проверку немедленно,*

нажмите на кнопку **Начать опрос**.

**Просмотр результатов опроса Active Directory**

► *Чтобы просмотреть результаты опроса Active Directory:*

1. В главном меню программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Active Directory**.

Отобразится список обнаруженных организационных подразделений.

2. Если вы хотите, выберите организационное подразделение и нажмите на кнопку **Устройства**.

Отобразится список устройств организационного подразделения.

Вы можете выполнить поиск устройств в списке и фильтровать результаты.

См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Опрос IP-диапазонов

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254.

Не рекомендуется использовать опрос IP-диапазонов, если вы используете опрос сети Windows и / или опрос Active Directory.

Kaspersky Security Center может опрашивать диапазоны IP-адресов путем обратного поиска DNS или по NBNS-протоколу:

- **Обратный поиск DNS.**

Kaspersky Security Center пытается выполнить обратное преобразование имен: для каждого IP-адреса из указанного диапазона выполнить преобразование в DNS-имя с помощью стандартных DNS-запросов. Если данная операция завершается успешно, сервер отправляет запрос `ICMP ECHO REQUEST` (аналог команды ping) на полученное имя. Если устройство отвечает, информация об этом устройстве добавляется в базу данных Kaspersky Security Center. Обратное преобразование имен необходимо для исключения сетевых устройств, которые могут иметь IP-адреса, но не являются компьютерами, таких как сетевые принтеры или роутеры.

Этот способ опроса основывается на правильно настроенной локальной службе DNS. Для его использования должна быть настроена зона обратного просмотра DNS. В сетях, в которых используется Active Directory, такая зона поддерживается автоматически. Но в таких сетях опрос IP-подсети не предоставляет дополнительной информации, помимо информации из опроса Active Directory. Кроме того, администраторы малых сетей часто не выполняют настройку зон обратного просмотра DNS, поскольку это не является необходимым для работы многих сетевых служб. Из-за этих причин опрос IP-подсети по умолчанию отключен.

- **NBNS-протокол.**

  Если обратное разрешение имен в вашей сети по каким-либо причинам невозможно, Kaspersky Security Center использует NBNS-протокол для опроса IP-диапазонов. Если запрос к IP-адресу возвращает NetBIOS-имя, информация об этом устройстве добавляется в базу данных Kaspersky Security Center.

Перед началом работы убедитесь, что SMB-протокол включен. Иначе Kaspersky Security Center не сможет обнаружить устройства в опрашиваемой сети. Чтобы включить протокол SMB, следуйте инструкциям для вашей операционной системы.

**Просмотр и изменение параметров опроса IP-диапазонов**

► *Чтобы просмотреть и изменить параметры опроса IP-диапазонов:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств опроса IP-диапазонов.
3. Включите или выключите опрос IP-диапазонов, используя переключатель **Разрешить опрос**.
4. Настройте расписание опроса. По умолчанию опрос IP-диапазонов запускается каждые 420 минут (семь часов).

   При указании интервала опроса убедитесь, что его значение не превышает значения параметра время действия IP-адреса (см. стр. 1061). Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

   Варианты расписания опроса:

   - **Каждые N дней**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр выключен.

5. Нажмите на кнопку **Сохранить**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

**Запуск опроса вручную**

► *Чтобы запустить проверку немедленно,*

нажмите на кнопку **Начать опрос**.

См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Добавление и изменение IP-диапазона

Исходно Kaspersky Security Center получает IP-диапазоны для опроса из сетевых параметров устройства, на которое он установлен. Если адрес устройства 192.168.0.1, а маска подсети – 255.255.255.0, Kaspersky Security Center автоматически включит сеть 192.168.0.0/24 в список адресов для опроса. Kaspersky Security Center выполнит опрос всех адресов от 192.168.0.1 до 192.168.0.254. Вы можете изменять автоматически определенные IP-диапазоны или добавлять собственные IP-диапазоны.

Вы можете создать диапазон только для IPv4-адресов. Если вы включите опрос Zeroconf (см. стр. 1063), Kaspersky Security Center будет опрашивать всю сеть.

► *Чтобы добавить новый IP-диапазон:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Чтобы добавить IP-диапазон, нажмите на кнопку **Добавить**.
3. В открывшемся окне настройте следующие параметры:
   - **Имя IP-диапазона**

     Имя IP-диапазона. Вы можете указать IP-диапазон по имени, например, 192.168.0.0/24.
   - **IP-интервал или адрес и маска подсети**

     Задайте IP-диапазон, указав либо начальный и конечный IP-адреса, либо адрес подсети и маску подсети. Можно также выбрать один из существующих диапазонов IP-адресов, нажав на кнопку **Обзор**.
   - **Время действия IP-адреса (ч)**

При задании этого параметра убедитесь, что он превышает значение интервала опроса, заданного в расписании опроса (см. стр. 1059). Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

1. Выберите **Разрешить опрос IP-диапазона**, если вы хотите опрашивать подсеть или интервал, который вы указали. В противном случае подсеть или интервал, которые вы добавили, не будут опрошены.
2. Нажмите на кнопку **Сохранить**.

IP-диапазон добавлен в список IP-диапазонов.

Вы можете запустить опрос для каждого IP-диапазона в отдельности, используя кнопку **Начать опрос**. После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

► *Чтобы добавить подсеть в существующий IP-диапазон:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на имя IP-диапазона, в который вы хотите добавить подсеть.
3. В появившемся окне нажмите на кнопку **Добавить**.
4. Укажите подсеть либо с помощью ее адреса и маски, либо задав первый и последний IP-адреса в IP-диапазоне. Или добавить существующую подсеть, нажав на кнопку **Обзор**.
5. Нажмите на кнопку **Сохранить**.

   Подсеть добавлена в IP-диапазон.
6. Нажмите на кнопку **Сохранить**.

Параметры IP-диапазона сохранены.

Вы можете добавить столько подсетей, сколько необходимо. Именованные IP-диапазоны не должны пересекаться, но на неименованные подсети внутри IP-диапазонов это ограничение не распространяется. Вы можете включить или отключить опрос независимо для каждого IP-диапазона.

См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Точка распространения может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и точка распространения опрашивает всю сеть, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, вы должны установить утилиту avahi-browse на точке распространения.

► *Чтобы включить опрос IPv6-сети:*

1. В главном меню программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **IP-диапазоны**.
2. Нажмите на кнопку **Свойства**.
3. В открывшемся окне включите переключатель **Использовать Zeroconf для опроса IPv6-сетей**.

После этого точка распространения начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

## Настройка правил хранения для нераспределенных устройств

После того как опрос сети Windows завершен, обнаруженные устройства помещаются в подгруппы группы администрирования Нераспределенные устройства. Эта группа администрирования находится по следующему пути: **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-домены**. Папка **Windows-домены** является родительской группой. Папка содержит дочерние группы, имена которых соответствуют доменам и рабочим группам, обнаруженным во время опроса. Родительская группа может также содержать группы администрирования мобильных устройств. Вы можете настроить правила хранения нераспределенных устройств для родительской группы администрирования и для каждой дочерней группы. Правила хранения не зависят от параметров обнаружения устройств и работают, даже если обнаружение устройств выключено.

Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически, вы можете сделать это только вручную. Если вам нужно удалить устройство с зашифрованным диском, сначала расшифруйте диск, а затем удалите устройство.

При удалении устройства с зашифрованным диском данные, необходимые для расшифровки диска, также удаляются. В этом случае вы сможете расшифровать диск только в том случае, если у пользователя устройства есть пароль на расшифровку и на устройстве все еще установлена программа безопасности, которая использовалась для шифрования диска, например Kaspersky Endpoint Security для Windows.

► *Чтобы настроить правила хранения нераспределенных устройств:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Windows-домены**.

2. Выполните одно из следующих действий:
   - Чтобы настроить параметры родительской группы, нажмите на кнопку **Свойства**.

     Откроется окно свойств Windows-домена.
   - Чтобы настроить параметры дочерней группы, нажмите на ее имя.

     Откроется окно свойств дочерней группы.
3. Настройте следующие параметры:
   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. По умолчанию этот параметр распространяется на дочерние группы. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.
   - **Наследовать из родительской группы**

     Если этот параметр включен, период хранения для устройств в текущей группе наследуется от родительской группы и не может быть изменен.

     Этот параметр доступен только для дочерних групп.

     По умолчанию параметр включен.
   - **Обеспечить принудительное наследование параметров для дочерних групп**

     Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

     По умолчанию параметр выключен.
4. Нажмите на кнопку **Принять**.

Ваши изменения сохранены и применены.

## См. также:

Сценарий: Обнаружение устройств в сети.....1054

# Программы "Лаборатории Касперского": лицензирование и активация

В сертифицированном состоянии программы активация лицензии возможно только с использованием файла ключа.

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых программ "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации программа формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

### См. также:



### В этом разделе



## Лицензирование управляемых программ

Программы "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждой из программ. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемой программы;
- с помощью задачи *Добавление лицензионного ключа* управляемой программы;
- активация управляемой программы вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Программа "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Программа, для которого

вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

**Автоматическое распространение**

Если вы используете разные управляемые программы и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Для всех ключей установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства**. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Windows. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Программа определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1* и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае нельзя предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение (см. стр. 341), таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 393).
  - Автоматическое распространение лицензионного ключа (см. стр. 395).

  Или
- Kaspersky Security Center 14.2 Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 1068).
  - Автоматическое распространение лицензионного ключа (см. стр. 1069).

**Добавление файла ключа или кода активации в инсталляционный пакет управляемой программы.**

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этой программы. Лицензионный ключ

распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции:

- Консоль администрирования:
  - Создание инсталляционного пакета (на стр. 372).
  - Установка программ на клиентские устройства (на стр. 810).

  Или
- Kaspersky Security Center 14.2 Web Console: Добавление лицензионного ключа в инсталляционный пакет (см. стр. 1029).

**Распространение с помощью задачи добавления лицензионного ключа управляемой программы**

В случае использования задачи *Добавление лицензионного ключа* управляемой программы вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Консоль администрирования:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 393).
  - Распространение лицензионного ключа на клиентские устройства (на стр. 395).

  Или
- Kaspersky Security Center 14.2 Web Console:
  - Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 1068).
  - Распространение лицензионного ключа на клиентские устройства (на стр. 1068).

**Добавление кода активации или файла ключа вручную на устройства.**

Вы можете активировать установленную программу "Лаборатории Касперского" локально, используя инструменты программы. Дополнительную информацию см. в документации к установленным программам.

## См. также

## Добавление лицензионного ключа в хранилище Сервера администрирования

► *Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:*

1. В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. Выберите то, что вы хотите добавить:
   - **Добавить файл ключа**

     Нажмите на кнопку **Выберите файл ключа** и выберите файл .key, который вы хотите добавить.
   - **Ввести код активации**

     Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.
4. Нажмите на кнопку **Закрыть**.

Лицензионный ключ или несколько лицензионных ключей добавлены в хранилище Сервера администрирования.

### См. также



## Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center 14.2 Web Console позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи *Распространение лицензионного ключа*.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования (см. стр. 1068).

► *Чтобы распространить лицензионный ключ на клиентские устройства:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи.

3. Выберите программу для которой вы хотите добавить лицензионный ключ.
4. В списке **Тип задачи** выберите **Добавить лицензионный ключ**.
5. Следуйте инструкциям мастера.
6. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Запустить**.

   Задача будет создана и отобразится в списке задач.
8. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Когда задача завершится, лицензионный ключ распространится на выбранные устройства.

### См. также


Лицензирование управляемых программ ..... 1065
Добавление лицензионного ключа в хранилище Сервера администрирования ..... 1068
Автоматическое распространение лицензионного ключа ..... 1069
Просмотр информации об используемых лицензионных ключах ..... 1070
Удаление лицензионного ключа из хранилища ..... 1071
Отзыв согласия с Лицензионным соглашением ..... 1072
Продление срока действия лицензии программ "Лаборатории Касперского" ..... 1074
Основной сценарий установки ..... 92
Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ..... 948
Лицензии и возможности Kaspersky Security Center ..... 69
Лицензирование управляемых программ ..... 390


## Автоматическое распространение лицензионного ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства:*

1. В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.
3. В открывшемся окне свойств лицензионного ключа установите флажок **Распространить лицензионный ключ на управляемые устройства**.
4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для программы при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Если вы установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**, соответствующий лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ (см. стр. 395).

### См. также


Лицензирование управляемых программ ..... 1065

Добавление лицензионного ключа в хранилище Сервера администрирования ..... 1068

Распространение лицензионного ключа на клиентские устройства ..... 1068

Просмотр информации об используемых лицензионных ключах ..... 1070

Удаление лицензионного ключа из хранилища ..... 1071

Отзыв согласия с Лицензионным соглашением ..... 1072

Продление срока действия лицензии программ "Лаборатории Касперского" ..... 1074

Основной сценарий установки ..... 92

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ..... 948

Лицензии и возможности Kaspersky Security Center ..... 69

Лицензирование управляемых программ ..... 390


## Просмотр информации об используемых лицензионных ключах

► *Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:*

В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

► *Чтобы просмотреть подробную информацию о ключе:*

1. В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На закладке **Общие** – основную информацию о лицензионном ключе.

- На закладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленной программы "Лаборатории Касперского".

► *Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства перейдите на закладку **Программы**.
4. Нажмите на название программы, для которой вы хотите просмотреть информацию о распространенном лицензионном ключе.
5. В открывшемся окне свойств программы перейдите на закладку **Общие** и откройте раздел **Лицензирование**.

Отобразится основная информация об активных и резервных лицензионных ключах.

Для определения актуальных параметров лицензионных ключей виртуального Сервера администрирования Сервер администрирования отправляет запрос на серверы активации "Лаборатории Касперского" не реже одного раза в сутки. Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871).

### См. также



## Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа для дополнительной возможности Сервера администрирования, например, для возможности Системного администрирования (см. стр. 353) или Управления мобильными устройствами (см. стр. 353), соответствующая функциональность становится недоступной. Если был добавлен резервный лицензионный ключ, он автоматически становится активным после удаления предыдущего активного лицензионного ключа.

При удалении активного лицензионного ключа, который распространен на управляемые устройства, программы продолжают работать на управляемых устройствах.

► *Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:*

1. Убедитесь, что Сервер администрирования не использует файл ключа или код активации, который вы хотите удалить. Если Сервер администрирования использует такой ключ, вы не сможете удалить ключ. Чтобы выполнить проверку:

   a. В главном меню нажмите на значок параметров (  ) рядом с именем требуемого Сервера администрирования.

      Откроется окно свойств Сервера администрирования.

   b. На закладке **Общие** выберите раздел **Лицензионные ключи**.

   c. Если в открывшемся разделе отображается нужный файл ключа или код активации, нажмите на кнопку **Удалить активный лицензионный ключ** и подтвердите операцию. После этого Сервер администрирования не использует удаленный лицензионный ключ, ключ остается в хранилище Сервера администрирования. Если требуемый файл ключа или код активации не отображается, Сервер администрирования его не использует.

2. В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.

3. Выберите нужный файл ключа или код активации, а затем нажмите на кнопку **Удалить**.

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить (см. стр. 1068) удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

### См. также



## Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любой управляемой программы "Лаборатории Касперского". Вам нужно удалить выбранную программу, прежде чем отзывать ее Лицензионное соглашение.

Лицензионные соглашения, принятые на виртуальном Сервере администрирования, можно отозвать на виртуальном Сервере администрирования или на главном Сервере администрирования. Лицензионные соглашения, принятые на главном Сервере администрирования, можно отозвать только на главном Сервере администрирования.

► *Чтобы отозвать Лицензионное соглашение для управляемых программ "Лаборатории Касперского":*

1. Откройте окно свойств Сервера администрирования и на закладке **Общие** выберите раздел **Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.

3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.
   - Полный текст Лицензионного соглашения.
   - Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

   В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить программу "Лаборатории Касперского", которой соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; программа больше не установлена.

См. также:



# Продление срока действия лицензии программ "Лаборатории Касперского"

Вы можете продлить срок действия лицензии программ "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

► *Чтобы продлить лицензии срок действия истекает или уже истек:*

1. Выполните одно из следующих действий:
   - В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
   - В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

   Откроется окно **Лицензии "Лаборатории Касперского"**, в котором вы можете просмотреть и продлить срок действия лицензии.
2. Перейдите по ссылке **Продлить лицензию** рядом с требуемой лицензией.

   Нажимая на ссылку продления срока действия лицензии, вы соглашаетесь передавать в "Лабораторию Касперского" следующие данные Kaspersky Security Center: версию, локализацию, которую вы используете, идентификатор лицензии на программное обеспечение (то есть идентификатор лицензии, которую вы продлеваете), а также то, приобрели ли вы лицензию через компанию-партнера или нет.
3. В открывшемся окне службы продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В Kaspersky Security Center 14.2 Web Console уведомления отображаются при приближении истечения срока действия лицензии по следующему расписанию:

- за 30 дней до истечения срока действия;
- за 7 дней до истечения срока действия;
- за 3 дней до истечения срока действия;

- за 24 часа до истечения срока действия;
- когда срок действия лицензии истек.

### См. также:



# Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

kaspersky

## См. также:



## В этом разделе



# Сценарий: Настройка защиты сети

Мастер первоначальной настройки создает политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться не оптимальными или даже запрещенными в организации. Поэтому рекомендуется настроить эти политики и задачи и создать дополнительные политики и задачи, если это необходимо для вашей сети.

**Предварительные требования**

Прежде чем приступать, убедитесь, что вы выполнили следующее:

- Установили Сервер администрирования Kaspersky Security Center (см. стр. 238).
- Установили Kaspersky Security Center 14.2 Web Console (см. стр. 950) (если требуется).
- Выполнили основной сценарий установки Kaspersky Security Center (см. стр. 92).

- Мастер первоначальной настройки (см. стр. 1007) завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования;
  - задача *Поиск уязвимостей и требуемых обновлений*.

Настройка защиты сети состоит из следующих этапов:

a. **Настройка и распространение политик и профилей политик для программ "Лаборатории Касперского"**

Для настройки и распространения параметров программ "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью (см. стр. 404): ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода. Для реализации ориентированного на устройства (см. стр. 402) метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center 14.2 Web Console. Для реализации ориентированного на пользователей (см. стр. 1081) метода управления безопасностью подходит только Kaspersky Security Center 14.2 Web Console.

b. **Настройка задач для удаленного управления программами "Лаборатории Касперского"**

Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

Инструкции:

Консоль администрирования:

Настройка групповой задачи обновления Kaspersky Endpoint Security (см. стр. 408).

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).

Kaspersky Security Center 14.2 Web Console:

Настройка групповой задачи обновления Kaspersky Endpoint Security (см. стр. 1104).

Параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

При необходимости создайте дополнительные задачи (см. стр. 411) управления программами "Лаборатории Касперского", установленными на клиентских устройствах.

c. **Оценка и ограничение загрузки событий в базу данных**

Информация о событиях в работе управляемых программ передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

Консоль администрирования: Настройка количества событий в хранилище событий (см. стр. 410).

Kaspersky Security Center 14.2 Web Console: Настройка количества событий в хранилище событий (см. стр. 983).

**Результаты**

После завершения этого сценария ваша сеть будет защищена благодаря настройке программ "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Программы "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление программами осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и программ "Лаборатории Касперского" (см. стр. 449).

Подробнее о настройке автоматического ответа на угрозы, обнаруженных Kaspersky Sandbox, см. в онлайн-справке Kaspersky Sandbox 2.0 https://support.kaspersky.com/KSB/2.0/ru-RU/189425.htm.

### См. также:



## Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры программ к разным устройствам, вы можете использовать один или оба типа управления в комбинации. Для реализации ориентированного на устройства метода управления безопасностью подходят средства Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) и Kaspersky Security Center 14.2 Web Console. Для реализации ориентированного на пользователей метода управления безопасностью подходит только Kaspersky Security Center 14.2 Web Console.

Управление безопасностью, ориентированное на устройства (см. стр. 402), позволяет вам применять различные параметры программы безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования. Вы также можете разграничить устройства по использованию этих устройств в Active Directory или по характеристикам аппаратного обеспечения.

Управление безопасностью, ориентированное на пользователя (см. стр. 1081), позволяет вам применять различные параметры программ безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры программы для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры программ к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с программами "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры программы могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры программ для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать инциденты безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или

сократить его права, чтобы изменить параметры программы. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик (см. стр. 1171) для одной или нескольких пользовательских ролей вашей организации. В этом случае политики и профили политик применяются в следующем порядке:

1. Применяются политики, созданные для управления безопасностью, ориентированного на устройства.
2. Они модифицируются профилями политик в соответствии с параметрами профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей (см. стр. 1224).

## См. также:

Сценарий: Настройка защиты сети .....400

# Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

### Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center (см. стр. 238) и Kaspersky Security Center 14.2 Web Console (см. стр. 950) (если требуется). Если вы установили Kaspersky Security Center 14.2 Web Console, вам может быть интересно также управление безопасностью (см. стр. 1081), ориентированное на пользователей, в качестве альтернативы или дополнения к управлению безопасностью, ориентированному на устройства.

### Этапы

Сценарий управления программами "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

#### a. Настройка политик программ

Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. стр. 1174) для каждой программы. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для следующих программ:

Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.

Kaspersky Endpoint Security для Linux – для клиентских устройств с операционной системой Linux

Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. стр. 405).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами

администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их в вышележащей политике. Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. 426) позволяет эффективно управлять устройствами в группах администрирования.

Инструкции:

Консоль администрирования: Создание политики (см. стр. 430)

Kaspersky Security Center 14.2 Web Console: Создание политики (см. стр. 1174)

**b. Создание профилей политики (если требуется)**

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики (см. стр. 1171) для этих устройств. Профиль политики представляет собой именованное подмножество параметров политики. Это подмножество параметров распространяется на устройства вместе с политикой и дополняет политику при выполнении определенного условия – *условия активации профиля*. Профили содержат только те параметры, которые отличаются от "базовой" политики, действующей на управляемом устройстве.

Используя условия активации профиля, вы можете применять различные профили политики, например, к устройствам, расположенным в определенном подразделении или группе безопасности Active Directory, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги (см. стр. 1159). Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *Windows*, назначить его всем устройствам под управлением операционной системы Windows, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы Windows установленные программы "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

Консоль администрирования:

Создание правила активации профиля политики (см. стр. 439).

Создание правила активации профиля политики (см. стр. 441).

Kaspersky Security Center 14.2 Web Console:

Создание профиля политики (см. стр. 1184).

Создание правила активации профиля политики (см. стр. 1186).

**c. Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно (см. стр. 726). Также синхронизация выполняется принудительно после создания или изменения политики или профиля политики. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам.

Если вы используете Kaspersky Security Center 14.2 Web Console, можно проверить, доставлены ли политики и профили политик на устройства. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции:

Консоль администрирования: Принудительная синхронизация (см. стр. 726).

Kaspersky Security Center 14.2 Web Console: Принудительная синхронизация (см. стр. 1272).

**Результаты**

После завершения сценария, ориентированного на устройства, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики программ и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

## См. также:


Основной сценарий установки....92

Иерархия Серверов администрирования....78

Группы администрирования....81

Политики....83

Профили политик....85

Иерархия политик....426

О ролях пользователей....1190

Сценарий: Настройка защиты сети....400


# Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке программ "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

Этот сценарий можно реализовать с помощью Kaspersky Security Center Web Console версии 13 и выше.

**Предварительные требования**

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center (см. стр. 238) и Kaspersky Security Center 14.2 Web Console (см. стр. 950) и завершили основной сценарий установки (см. стр. 92). Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства (см. стр. 402) как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению (см. стр. 404).

**Процесс**

Сценарий управления программами "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

a. **Настройка политик программ**

Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. стр. 429) для каждой программы. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс

настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы. Перейдите к настройке политики Kaspersky Endpoint Security вручную (см. стр. 1098).

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики (см. стр. 1168). Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. 1170) позволяет эффективно управлять устройствами в группах администрирования.

Инструкции: Создание политики (см. стр. 1174)

**b. Укажите пользователей в качестве владельцев устройств**

Назначьте управляемым устройствам соответствующие роли.

Инструкции: Назначение пользователя владельцем устройства (см. стр. 1220).

**c. Определение пользовательских ролей, типичных для вашей организации**

Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вы должны разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры программы, специфичные для этой роли.

**d. Создание пользовательских ролей**

Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям программы.

Инструкции: Создание роли пользователя (см. стр. 1222).

**e. Определение области для каждой роли пользователя**

Для каждой созданной роли пользователя определите пользователей и / или группы безопасности и группы администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Инструкции: Изменение области для роли пользователя (см. стр. 1223).

**f. Создание профиля политики**

Создайте профиль политики (см. стр. 1171) для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к программам, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

Инструкции: Создание профиля политики (см. стр. 1184).

**g. Связь профиля политики с ролями пользователей**

Свяжите профиль профиля политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к программам "Лаборатории Касперского", установленным на устройствах пользователя.

Инструкции: Связь профилей политики с ролями (см. стр. 1224).

**h. Распространение политик и профилей политик на управляемые устройства**

По умолчанию синхронизация управляемых устройств с Сервером администрирования происходит раз в 15 минут. Во время синхронизации новые или измененные политики и профили политик применяются к управляемым устройствам. Вы можете пропустить автоматическую синхронизацию и запустить синхронизацию вручную с помощью команды Синхронизировать принудительно. После завершения синхронизации политики и профили политик доставляются и применяются к установленным программам "Лаборатории Касперского".

Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

Инструкции: Принудительная синхронизация (см. стр. 1272).

**Результаты**

После завершения сценария, ориентированного на пользователя, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики программ и профили политик будут автоматически применяться к устройствам этого пользователя.

### См. также:



## Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на имя политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

Обратите внимание, что для устройств под управлением Windows, macOS и Linux, доступны различные параметры (см. стр. 1096).

**Общие**

На этой закладке можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:

- **Активная**

  Если выбран этот вариант, политика становится активной.

  По умолчанию выбран этот вариант.

- **Неактивная**

  Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.

- В блоке **Наследование параметров** можно настроить параметры наследования политики:

  - **Наследовать параметры из политики верхнего уровня**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

**Настройка событий**

На этой закладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на закладке **Настройка событий**:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке типов событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений (на стр. 316), указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в раздел **Предупреждение** вы можете настроить тип события **Произошел инцидент**. Такие события могут произойти, например, когда свободное место на диске точки распространения (см. стр. 88) меньше 2 ГБ (для установки программ и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошел инцидент**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаружил инцидент, вы можете управлять этим инцидентом с помощью параметров управляемого устройства (см. стр. 742).

**Параметры программы**

**Параметры**

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Распространять файлы только через точки распространения**

  Если этот параметр включен, Агенты администрирования на управляемых устройствах получают обновления только от точек распространения.

  Если этот параметр выключен, Агенты администрирования на управляемых устройствах получают обновления от точек распространения или от Сервера администрирования (см. стр. 453).

Обратите внимание, что программы безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждой программы безопасности. Если вы включили параметр **Распространять файлы только через точки распространения**, убедитесь, что Kaspersky Security Center установлен в качестве источника обновлений в задачах обновления.

  По умолчанию параметр выключен.

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Программа может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в программу безопасности (например, Kaspersky Endpoint Security для Windows). Передаваемая информация отображается в интерфейсе программы безопасности.

  Агент администрирования передает следующую информацию:

- время доставки политики на управляемое устройство;
- имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
- имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
- список активных профилей политики.

  Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

- **Защитить службу Агента администрирования от неавторизованного удаления, остановки или изменения параметров работы**

Если этот параметр включен, после того как Агент администрирования был установлен на управляемом устройстве, компонент не может быть удален или изменен без необходимых прав. Работа Агента администрирования не может быть остановлена. Этот параметр не влияет на контроллеры домена.

Включите этот параметр, чтобы защитить Агент администрирования на рабочих станциях, управляемых с правами локального администратора.

По умолчанию параметр выключен.

- **Использовать пароль деинсталляции**

  Если параметр включен, при нажатии на кнопку **Изменить** можно указать пароль для задачи удаленной деинсталляции Агента администрирования.

  По умолчанию параметр выключен.

**Хранилища**

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

- **Информация об установленных программах**

  Если этот параметр включен, на Сервер администрирования отправляется информация о программах, установленных на клиентских устройствах.

  По умолчанию параметр включен.

- **Включить информацию о патче**

  Информация о патчах программ, установленных на клиентских устройствах, отправляется на Сервер администрирования. Включение этого параметра может увеличить нагрузку на Сервер администрирования и СУБД, а также вызвать увеличение объема базы данных.

  По умолчанию параметр включен. Доступен только для Windows.

- **Информация об обновлениях Центра обновления Windows**

  Если параметр установлен, на Сервер администрирования отправляется информация об обновлениях Центра обновления Windows, которые необходимо установить на клиентских устройствах.

  Иногда, даже если параметр выключен, обновления отображаются в свойствах устройства в разделе **Применимые обновления**. Это может произойти, если, например, устройства организации имеют уязвимости, которые могут быть закрыты с помощью этих обновлений.

  По умолчанию параметр включен. Доступен только для Windows.

- **Информация об уязвимостях программного обеспечения**

  Если этот параметр включен, информация об уязвимостях в программах сторонних производителей (включая программное обеспечение Microsoft), обнаруженных на управляемых устройствах, и об обновлениях программного обеспечения для устранения уязвимостей (не включая программное обеспечение Microsoft) отправляется на Сервер администрирования.

  Выбор этого параметра (**Информация об уязвимостях программного обеспечения**) увеличивает нагрузку на сеть, загрузку диска Сервера администрирования и потребление ресурсов Агентом администрирования.

По умолчанию параметр включен. Доступен только для Windows.

Для управления обновлениями программного обеспечения Microsoft используйте параметр **Информация об обновлениях Центра обновления Windows**.

- **Информация о реестре оборудования**

Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить сведения об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора.

**Обновления и уязвимости в программах**

В разделе **Обновления и уязвимости в программах** можно настроить поиск и распространение обновлений Windows, а также включить проверку исполняемых файлов на наличие уязвимостей: Параметры раздела **Обновления и уязвимости в программах** доступны только для устройств под управлением Windows:

- **Использовать Сервер администрирования в роли WSUS-сервера**

  Если этот параметр включен, обновления Windows загружаются на Сервер администрирования. Загруженные обновления Сервер администрирования централизованно предоставляет службам Windows Update на клиентских устройствах с помощью Агентов администрирования.

  Если этот параметр выключен, Сервер администрирования не используется для загрузки обновлений Windows. В этом случае клиентские устройства получают обновления Windows самостоятельно.

  По умолчанию параметр выключен.

- Вы можете ограничить обновления Центра обновления Windows, которые могут устанавливать пользователи на своих устройствах вручную, используя Центр обновления Windows.

  Для устройств с операционными системами Windows 10, если в Центре обновления Windows уже найдены обновления для устройств, то новый параметр, который вы выбрали под **Разрешить пользователям управлять установкой обновлений Центра обновления Windows**, будет применен только после установки найденных обновлений.

  Выберите параметр из раскрывающегося списка:

  - **Устанавливать все применимые обновления Центра обновления Windows**

    Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам.

    Выберите этот вариант, если вы не хотите влиять на установку обновлений.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Устанавливать только одобренные обновления Центра обновления Windows**

Пользователи могут установить все обновления Центра обновления Windows, которые применимы к их устройствам и которые одобрены администратором.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом разрешить установку этих одобренных обновлений на клиентских устройствах.

Когда пользователь устанавливает обновления Центра обновления Windows вручную, обновления могут быть загружены с серверов Microsoft, а не с Сервера администрирования. Это возможно, если Сервер администрирования еще не загрузил эти обновления. Загрузка обновлений с серверов Microsoft приводит к увеличению трафика.

- **Запретить устанавливать обновления Центра обновления Windows**

Пользователи не могут устанавливать обновления Центра обновления Windows на своих устройства вручную. Все применимые обновления устанавливаются в соответствии с настройкой, заданной администратором.

Выберите этот вариант, если вы хотите централизованно управлять установкой обновлений.

Например, вы можете настроить расписание обновления так, чтобы не загружать сеть. Вы можете запланировать обновления вне рабочего времени, чтобы они не мешали производительности пользователей.

- В блоке параметров **Режим поиска обновлений Windows Update** можно выбрать режим поиска обновлений:
  - **Активный**

Если выбран этот вариант, Сервер администрирования с помощью Агента администрирования инициирует обращение агента обновлений Windows на клиентском устройстве к источнику обновлений: Windows Update Servers или WSUS. Далее Агент администрирования передает на Сервер администрирования информацию, полученную от Агента Центра обновления Windows.

Этот параметр вступает в силу только в том случае, если параметр **Соединяться с сервером обновлений для актуализации данных** задачи *Поиск уязвимостей и требуемых обновлений* включен.

По умолчанию выбран этот вариант.

  - **Пассивный**

Если выбран этот вариант, Агент администрирования периодически передает на Сервер администрирования информацию об обновлениях, полученную при последней синхронизации агента обновлений Windows с источником обновления. Если синхронизация агента обновлений Windows с источником обновления не выполняется, данные об обновлениях на Сервере администрирования устаревают.

Выберите этот параметр, если вы хотите получать обновления из кеша источника обновлений.

  - **Выключен**

Если выбран этот вариант, Сервер администрирования не запрашивает

информацию об обновлениях.

Выберите этот параметр, если, например, вы хотите сначала протестировать обновления на локальном устройстве.

- **Проверять исполняемые файлы на наличие уязвимостей при запуске**

  Если параметр включен, при запуске исполняемых файлов выполняется их проверка на наличие уязвимостей.

  По умолчанию параметр включен.

**Управление перезагрузкой**

В разделе **Управление перезагрузкой** можно выбрать и настроить действие, если в ходе работы, установки или удаления программы требуется перезагрузка операционной системы управляемого устройства. Параметры раздела **Управление перезагрузкой** доступны только для устройств под управлением Windows:

- **Не перезагружать операционную систему**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **При необходимости перезагрузить операционную систему автоматически**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Периодичность напоминания о необходимости установки (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагружать через (мин)**

    После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

**Совместный доступ к рабочему столу Windows**

В разделе **Совместный доступ к рабочему столу Windows** можно включить и настроить аудит действий администратора на удаленном устройстве пользователя при использовании общего доступа к рабочему столу: Параметры раздела **Совместный доступ к рабочему столу Windows** доступны только для устройств под управлением Windows:

- **Включить аудит**

  Если параметр включен, аудит действий администратора на удаленном устройстве включен. Записи о действиях администратора на удаленном устройстве сохраняются:

  - в журнале событий на удаленном устройстве;
  - в файле с расширением syslog, который находится в папке установки Агента администрирования на удаленном устройстве;
  - в базе событий Kaspersky Security Center.

  Аудит действий администратора доступен при выполнении следующих условий:

  - лицензия на Системное администрирование уже используется;
  - у администратора есть право на запуск общего доступа к рабочему столу удаленного устройства.

  Если параметр выключен, аудит действий администратора на удаленном устройстве выключен.

  По умолчанию параметр выключен.

- **Маски файлов, чтение которых нужно отслеживать**

  В списке содержатся маски файлов. Когда аудит включен, программа отслеживает чтение администратором файлов, соответствующих маскам, и сохраняет информацию о чтении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

  По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Маски файлов, изменение которых нужно отслеживать**

  В списке содержатся маски файлов на удаленном устройстве. Когда аудит включен,

программа отслеживает изменение администратором файлов, соответствующих маскам, и сохраняет информацию об изменении файлов. Список доступен, когда установлен флажок **Включить аудит**. Можно изменять маски файлов и добавлять в список новые маски. Новые маски файлов нужно указывать в списке с новой строки.

По умолчанию указаны маски файлов *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

**Управление патчами и обновлениями**

В разделе **Управление патчами и обновлениями** можно настроить получение и распространение обновлений и установку патчей на управляемые устройства:

- **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**

  Если флажок установлен, патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений.

  Если параметр выключен, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

  По умолчанию параметр включен.

- **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**

  Если флажок снят, офлайн-модель получения обновлений выключена. Когда Сервер администрирования получает обновления, он уведомляет Агент администрирования (на устройствах, где он установлен) об обновлениях, которые потребуются для управляемых программ. Когда Агенты администрирования получают информацию об обновлениях, они загружают нужные файлы с Сервера администрирования заранее. При первом соединении с Агентом администрирования Сервер инициирует загрузку обновлений этим Агентом. После того как Агент администрирования на клиентском устройстве загрузит все обновления, обновления становятся доступными для программ на устройстве.

  Когда управляемая программа на клиентском устройстве обращается к Агенту администрирования за обновлениями, Агент проверяет, есть ли у него необходимые обновления. Если обновления были получены от Сервера администрирования не раньше, чем за 25 часов с момента запроса управляемой программы, Агент администрирования не подключается к Серверу администрирования и предоставляет управляемой программе обновления из локального кеша. Соединение с Сервером администрирования может не выполняться, когда Агент администрирования предоставляет обновления для программ на клиентских устройствах, но подключение не требуется для обновления.

  Если параметр выключен, офлайн-модель получения обновлений не используется. Обновления распространяются в соответствии с расписанием задачи загрузки обновлений.

  По умолчанию параметр включен.

**Подключения**

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**

- **Профили соединений**
- **Расписание соединений**

В разделе **Подключения** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключение к Серверу администрирования** можно настроить параметры подключения к Серверу администрирования и указать период синхронизации клиентских устройств с Сервером администрирования:
  - **Период синхронизации (мин)**

    Агент администрирования синхронизирует управляемые устройства с Сервером администрирования. Рекомендуется задать период синхронизации (периодический сигнал (см. стр. 176)) равным 15 минут на 10 000 управляемых устройств.

    Если установлен период синхронизации меньше 15 минут, то синхронизация выполняется каждые 15 минут. Если период синхронизации установлен на 15 минут или более, синхронизация выполняется с указанным периодом.
  - **Сжимать сетевой трафик**

    Если параметр выключен, будет увеличена скорость передачи данных Агентом администрирования, сокращен объем передаваемой информации и уменьшена нагрузка на Сервер администрирования.

Нагрузка на центральный процессор клиентского компьютера может возрасти.

По умолчанию флажок установлен.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если параметр включен, UDP-порт, необходимый для работы Агента администрирования, будет добавлен в список исключений сетевого экрана Microsoft Windows.

  По умолчанию параметр включен.
- **Использовать SSL-соединение**

  Если этот параметр включен, подключение к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

  По умолчанию параметр включен.
- **Использовать шлюз соединений точки распространения (при наличии) в параметрах подключения по умолчанию**

  Если параметр включен, то используется шлюз соединений точки распространения, параметры которой заданы в свойствах группы администрирования.

  По умолчанию параметр включен.

- **Использовать UDP-порт**

  Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

  Если клиентское устройство работает под управлением операционной системы Windows XP Service Pack 2, встроенный сетевой экран блокирует UDP-порт с номером 15000. Этот порт требуется открыть вручную.

- **Использовать точку распространения для принудительного подключения к Серверу администрирования**

В подразделе **Профили подключения** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows и macOS:

- **Параметры сетевого местоположения**

Параметры сетевого местоположения определяют характеристики сети, к которой подключено клиентское устройство, и задают правила переключения Агента администрирования с одного профиля подключения Сервера администрирования на другой при изменении характеристик сети.

- **Профили подключения к Серверу администрирования**

В этом разделе можно просмотреть и добавить профили подключения Агента администрирования к Серверу администрирования. В этом разделе также можно сформировать правила переключения Агента администрирования на другие Серверы администрирования при возникновении следующих событий:

- подключении клиентского устройства к другой локальной сети;
- отключении устройства от локальной сети организации;
- изменении адреса шлюза соединения или изменении адреса DNS-сервера.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если параметр включен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей (см. стр. 310). В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

  Если параметр выключен, программы будут использовать активные политики.

  По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

**Опрос сети точками распространения**

В подразделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Параметры опроса сети доступны только для устройств под управлением Windows. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Сеть Windows**

  Если параметр включен, Сервер администрирования автоматически опрашивает сеть в соответствии с расписанием, настроенным по ссылкам **Настроить расписание быстрого опроса** и **Настроить расписание полного опроса**.

Если этот параметр выключен, Сервер администрирования опрашивает сеть с указанным периодом в поле **Период опроса сети (мин)**.

  Период обнаружения устройств для версий Агента администрирования версий ниже 10.2 можно настроить в полях **Период опроса Windows-доменов (мин)** и **Период опроса сети (мин)**.

  По умолчанию параметр выключен.

- **Zeroconf**
- **IP-диапазоны**

  Если параметр включен, Сервер администрирования автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если этот параметр выключен, точка распространения не выполняет опрос IP-диапазонов.

  Периодичность опроса IP-диапазонов для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если параметр включен.

  По умолчанию параметр выключен.

- **Active Directory**

  Если параметр включен, Сервер администрирования автоматически выполняет опрос Active Directory в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если параметр выключен, точка не выполняет опрос Active Directory.

  Периодичность опроса Active Directory для версий Агента администрирования версий ниже 10.2 можно настроить в поле **Период опроса (мин)**. Поле доступно, если этот параметр включен.

  По умолчанию параметр выключен.

**Параметры сети для точек распространения**

В разделе **Параметры сети для точек распространения** можно настроить параметры доступа к интернету:

- **Использовать прокси-сервер**
- **Адрес**
- **Номер порта**
- **Не использовать прокси-сервер для локальных адресов**

  Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

  По умолчанию параметр выключен.

- **Аутентификация на прокси-сервере**

  Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

  По умолчанию флажок снят.

- **Имя пользователя**
- **Пароль**

**Прокси-сервер KSN (точки распространения)**

В разделе **Прокси-сервер KSN (точки распространения)** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки Kaspersky Security Network (KSN) запросов от управляемых устройств:

- **Включить прокси-сервер KSN на стороне точки распространения**

  Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и оптимизации трафика сети.

  Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены (см. стр. 830) в окне свойств Сервера администрирования.

  Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Переслать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной-службе KSN / Локальному KSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или Локальному KSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или Локальный KSN.

Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к Локальному KSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения.

Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к Локальному KSN.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

  Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

**Обновления (точки распространения)**

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий (см. стр. 459), так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского".

**История ревизий**

На этой закладке вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат (см. стр. 1108).

## См. также:



## Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования (см. стр. 1083) можно использовать для настройки Агента администрирования для конкретной операционной системы.

*Таблица 86. Параметры политики Агента администрирования: сравнение по операционным системам*

| Раздел Политики | Windows | macOS | Linux |
|---|---|---|---|
| **Общие** | ✓ | ✓ | ✓ |
| **Настройка событий** | ✓ | ✓ | ✓ |
| **Параметры** | ✓ | ✓ | ✓<br>Доступны только параметры **Максимальный размер очереди событий (МБ)** и **Программа может получать расширенные данные политики на устройстве**. |
| **Хранилища** | ✓ | — | ✓<br>Доступны только параметры **Информация об установленных программах** и **Информация о реестре оборудования**. |
| **Обновления и уязвимости в программах** | ✓ | — | — |
| **Управление перезагрузкой** | ✓ | — | — |
| **Совместный доступ к рабочему столу Windows** | ✓ | — | — |
| **Управление патчами и обновлениями** | ✓ | — | — |
| **Подключения → Сеть** | ✓ | ✓ | ✓<br>Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** |
| **Подключения → Профили соединений** | ✓ | ✓ | — |
| **Подключения → Расписание соединений** | ✓ | ✓ | ✓ |

| Раздел Политики | Windows | macOS | Linux |
|---|---|---|---|
| **Опрос сети точками распространения** | ✓ Доступны только параметры **Сеть Windows**, **IP-диапазоны** и **Active Directory**. | — | ✓ Доступны только параметры **Zeroconf** и **IP-диапазоны**. |
| **Параметры сети для точек распространения** | ✓ | ✓ | ✓ |
| **Прокси-сервер KSN (точки распространения)** | ✓ | — | ✓ |
| **Обновления (точки распространения)** | ✓ | — | ✓ |
| **История ревизий** | ✓ | ✓ | ✓ |

См. также:

Использование Агента администрирования для Windows, macOS и Linux: сравнение .....935

## Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security. Вы можете выполнить настройку в окне свойств политики. При изменении параметра, нажмите на значок замка справа от соответствующей группы параметров, чтобы применить указанные значения к рабочей станции.

## См. также:



## В этом разделе



## Настройка Kaspersky Security Network

Kaspersky Security Network (KSN) – инфраструктура облачных служб, обладающая информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network позволяет Kaspersky Endpoint Security для Windows быстрее реагировать на различные виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Подробнее о Kaspersky Security Network см. документацию Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/177936.htm.

► *Чтобы задать рекомендуемые параметры KSN:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите в раздел **Параметры программы** → **Продвинутая защита** → **Kaspersky Security Network**.
4. Убедитесь, что параметр **Использовать прокси-сервер KSN** включен. Использование этого параметра поможет перераспределить и оптимизировать трафик сети.
5. Если служба прокси-сервера KSN недоступна, можно включить использование серверов KSN (если требуется). Серверы KSN могут располагаться как на стороне "Лаборатории Касперского" (при использовании Глобального KSN), так и у третьих сторон (при использовании Локального KSN).
6. Нажмите на кнопку **ОК**.

Рекомендованные параметры KSN настроены.

## См. также:



## Проверка списка сетей, которые защищает сетевой экран

Убедитесь, что сетевой экран Kaspersky Endpoint Security для Windows защищает все ваши сети. По умолчанию сетевой экран защищает сети со следующими типами подключения:

- **Общедоступная сеть**. Антивирусные программы, сетевые экраны или фильтры не защищают устройства в такой сети.
- **Локальная сеть**. Доступ к файлам и принтерам ограничен для устройств в этой сети.
- **Доверенная сеть**. Устройства в такой сети защищены от атак и несанкционированного доступа к файлам и данным.

Если вы настроили пользовательскую сеть, убедитесь, что сетевой экран защищает ее. Для этого проверьте список сетей в свойствах политики Kaspersky Endpoint Security для Windows. В списке могут отображаться не все сети.

Подробнее о сетевом экране см. документацию Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/176738.htm.

► *Чтобы проверить список сетей:*

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В свойствах политики перейдите в раздел **Параметры программы → Базовая защита → Сетевой экран**.
4. В блоке **Доступные сети** перейдите по ссылке **Параметры сети**.

   Отобразится окно **Сетевые подключения**. В этом окне отобразится список сетей.
5. Если в списке отсутствует сеть, добавьте ее.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Выключение проверки сетевых устройств

Проверка сетевых дисков программой Kaspersky Endpoint Security для Windows, может оказывать на них значительную нагрузку. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Вы можете выключить проверку сетевых дисков в свойствах политики Kaspersky Endpoint Security для Windows. Полное описание этих параметров приведено в документации Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/176733.htm.

► *Чтобы выключить проверку сетевых дисков:*

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите в раздел **Параметры программы → Базовая защита → Защита от файловых угроз**.
4. В блоке **Область защиты**, выключите параметр **Все сетевые диски**.
5. Нажмите на кнопку **ОК**.

Проверка сетевых дисков выключена.

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Исключение сведений о программном обеспечении из памяти Сервера администрирования

Рекомендуется, настроить Сервер администрирования так, чтобы он не сохранял информацию о программных модулях, запущенных на сетевых устройствах. В результате память Сервера администрирования не переполняется.

Вы можете выключить сохранение этой информации в свойствах политики Kaspersky Endpoint Security для Windows.

► *Чтобы выключить сохранение информации об установленных программных модулях:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.
3. В окне свойств политики перейдите **Параметры программы** → **Общие параметры** → **Отчеты и хранилища**.
4. В блоке **Информировать Сервер администрирования**, снимите флажок **О запускаемых программах**, если он установлен в политике верхнего уровня.

   Когда этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех программных модулей на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов).

Информация об установленных программных модулях больше не сохраняется в базе данных Сервера администрирования.

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Настройка доступа к интерфейсу Kaspersky Endpoint Security для Windows на рабочих станциях

Если антивирусной защитой в сети организации требуется управлять централизованно через Kaspersky Security Center, укажите параметры интерфейса в свойствах политики Kaspersky Endpoint Security для Windows, как описано ниже. В результате вы предотвратите несанкционированный доступ к Kaspersky Endpoint Security для Windows на рабочих станциях и изменение параметров Kaspersky Endpoint Security для Windows.

Полное описание этих параметров приведено в документации Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/11.5.0/ru-RU/178492.htm.

► *Чтобы задать рекомендуемые параметры интерфейса:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.

2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.

3. В свойствах политики перейдите в раздел **Параметры программы** → **Общие параметры** → **Интерфейс**.

4. В блоке **Взаимодействие с пользователем** выберите параметр **Без интерфейса**. Отображение пользовательского интерфейса Kaspersky Endpoint Security для Windows на рабочих станциях будет выключено, и их пользователи не могут изменять параметры Kaspersky Endpoint Security для Windows.

5. В блоке **Включить защиту паролем** включите переключатель. Это снижает риск несанкционированного или непреднамеренного изменения параметров Kaspersky Endpoint Security для Windows на рабочих станциях.

Рекомендуемые параметры интерфейса Kaspersky Endpoint Security для Windows заданы.

## См. также:

Сценарий: Настройка защиты сети .....400

## Сохранение важных событий политики в базе данных Сервера администрирования

Чтобы избежать переполнения базы данных Сервера администрирования, рекомендуется сохранять в базе данных только важные события.

► *Чтобы настроить регистрацию важных событий в базе данных Сервера администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.

3. В окне свойств политики перейдите на закладку **Настройка событий**.
4. В разделе **Критические** нажмите на кнопку **Добавить события** и установите флажок только рядом со следующими событиями:
   - *Нарушено Лицензионное соглашение.*
   - *Автозапуск программы выключен.*
   - *Ошибка активации.*
   - *Обнаружена активная угроза. Требуется запуск процедуры лечения.*
   - *Лечение невозможно.*
   - *Обнаружена ранее открытая опасная ссылка.*
   - *Процесс завершен.*
   - *Сетевая активность запрещена.*
   - *Обнаружена сетевая атака.*
   - *Запуск программы запрещен.*
   - *Доступ запрещен (на основе локальных параметров).*

- *Доступ запрещен (KSN).*
- *Локальная ошибка обновления.*
- *Невозможен запуск двух задач одновременно.*
- *Ошибка взаимодействия с Kaspersky Security Center.*
- *Обновлены не все компоненты.*
- *Ошибка применения правил шифрования / расшифровки файлов.*
- *Ошибка активации портативного режима.*
- *Ошибка деактивации портативного режима.*
- *Не удалось загрузить модуль шифрования.*
- *Политика не может быть применена.*
- *Ошибка при изменении компонентов программы.*

5. Нажмите на кнопку **ОК**.
6. В разделе **Отказ функционирования** нажмите на кнопку **Добавить события** и установите флажок только рядом с событием *Неверные параметры задачи*. *Параметры задачи не применены*.
7. Нажмите на кнопку **ОК**.
8. В разделе **Предупреждение** нажмите на кнопку **Добавить события** и установите флажок только рядом со следующими событиями:
   - *Самозащита программы выключена.*
   - *Компоненты защиты выключены.*
   - *Недопустимый резервный ключ.*
   - *Обнаружено легальное ПО, которое может быть использовано для нанесения вреда компьютеру или персональным данным (на основе локальных параметров).*
   - *Обнаружено легальное ПО, которое может быть использовано для нанесения вреда компьютеру или персональным данным (KSN).*
   - *Объект удален.*
   - *Объект вылечен.*
   - *Пользователь отказался от политики шифрования.*
   - *Файл восстановлен из KATA-карантина.*
   - *Файл помещен на KATA-карантин.*
   - *Сообщение администратору о запрете запуска программы.*
   - *Сообщение администратору о запрете доступа к устройству.*
   - *Сообщение администратору о запрете доступа к веб-странице.*
9. Нажмите на кнопку **ОК**.
10. В разделе **Информационные сообщения** нажмите на кнопку **Добавить события** и установите флажок только рядом со следующим событием:
    - *Создана резервная копия объекта.*
    - *Запуск программы запрещен в тестовом режиме.*

11. Нажмите на кнопку **ОК**.

Регистрация важных событий в базе данных Сервера администрирования настроена.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальным и рекомендуемым расписанием для Kaspersky Endpoint Security является **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств

В компоненте Контроль устройств политики Kaspersky Endpoint Security для Windows вы можете управлять доступом пользователей к внешним устройствам, которые установлены или подключены к клиентскому устройству (например, жестким дискам, камерам или модулям Wi-Fi). Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.

Если вам необходимо предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств, но невозможно добавить устройство в список доверенных устройств, вы можете предоставить временный автономный доступ к внешнему устройству. Автономный доступ означает, что клиентское устройство не имеет доступа к сети.

Вы можете предоставить автономный доступ к внешнему устройству, заблокированному Контролем устройств, только если параметр **Разрешать запрашивать временный доступ** включен в параметрах политики Kaspersky Endpoint Security для Windows, в разделе **Параметры программы → Контроль безопасности → Контроль программ**.

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств, включает в себя следующие этапы:

1. В диалоговом окне Kaspersky Endpoint Security для Windows пользователь устройства, который хочет получить доступ к заблокированному внешнему устройству, формирует файл запроса доступа и отправляет его администратору Kaspersky Security Center.
2. Получив этот запрос, администратор Kaspersky Security Center создает файл ключа доступа и отправляет его пользователю устройства.
3. В диалоговом окне Kaspersky Endpoint Security для Windows пользователь устройства активирует файл ключа доступа и получает временный доступ к внешнему устройству.

► *Чтобы предоставить временный доступ к внешнему устройству, заблокированному компонентом Контроль устройств:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке выберите пользовательское устройство, которое запрашивает доступ к внешнему устройству, заблокированному компонентом Контроль устройств.

   Можно выбрать только одно устройство.

3. Нажмите на кнопку ( ••• ) над списком управляемых устройств, а затем на кнопку **Предоставить доступ к устройству в автономном режиме**.

4. В открывшемся окне **Параметры программы** в разделе **Контроль устройств** нажмите на кнопку **Обзор**.

5. Выберите файл запроса доступа, который вы должны получить от пользователя и нажмите на кнопку **Открыть**. Файл должен иметь формат AKEY.

   Отображается информация о заблокированном устройстве, к которому пользователь запросил доступ.

6. Укажите значение параметра **Длительность доступа к устройству**.

   Этот параметр определяет продолжительность времени, в течение которого вы предоставляете пользователю доступ к заблокированному устройству. Значением по умолчанию является значение, указанное пользователем при создании файла запроса доступа.

7. Укажите значение параметра **Период активации**.

   Этот параметр определяет период, в течение которого пользователь может активировать доступ к заблокированному устройству с помощью предоставленного ключа доступа.

8. Нажмите на кнопку **Сохранить**.

   Откроется стандартное окно Microsoft Windows **Сохранение ключа доступа**.

9. Выберите папку назначения, в которой вы хотите сохранить файл, содержащий ключ доступа для заблокированного устройства.

10. Нажмите на кнопку **Сохранить**.

В результате, когда вы отправляете пользователю файл ключа доступа и он активирует его в диалоговом окне Kaspersky Endpoint Security для Windows, пользователь получает временный доступ к заблокированному устройству на определенный период.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Удаленная деинсталляция программ или обновлений программного обеспечения

► *Чтобы удаленно деинсталлировать программы или обновления программного обеспечения:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Для программы Kaspersky Security Center выберите тип задачи **Удаленная деинсталляция программы**.
4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите, какую программу вы хотите деинсталлировать, а затем выберите требуемые программы, обновления или патчи, которые вы хотите удалить:
   - **Удалить управляемую программу**
   - **Удалить несовместимую программу**
   - **Удалить программу из реестра программ**
   - **Удалить указанное обновление программы, патч или стороннюю программу**
7. Укажите, как клиентские устройства будут загружать утилиту удаления:
   - **С помощью Агента администрирования**
   - **Средствами Microsoft Windows с помощью Сервера администрирования**
   - **Средствами операционной системы с помощью точек распространения**
   - **Максимальное количество одновременных загрузок**
   - **Максимальное количество попыток деинсталляции**
   - **Предварительно проверять тип операционной системы перед загрузкой**
8. Укажите параметры перезагрузки операционной системы:
   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.
   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).
   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

   - **Учетная запись не требуется (установлен Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

     Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

   - **Учетная запись требуется (установка без Агента администрирования)**

2. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

3. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

4. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

5. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112).

6. Нажмите на кнопку **Сохранить**.

7. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с выбранных устройств.

См. также:

Замещение программ безопасности сторонних производителей ..... 360
Сценарий: Настройка защиты сети ..... 400

## Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

► *Чтобы откатить изменения объекта:*

1. В окне свойств объекта перейдите на закладку **История ревизий**.
2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.
3. Нажмите на кнопку **Откатить**.
4. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Произойдет откат к выбранной ревизии. В списке ревизий объекта отобразится запись о выполненном действии. В описании ревизии отобразится информация о номере ревизии, к которой вы вернули объект.

Операция отката доступна только для политик и задач.

См. также:

Сценарий: Настройка защиты сети ..... 400

## Задачи

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

kaspersky

## См. также:



## В этом разделе



# О задачах

Kaspersky Security Center управляет работой программ "Лаборатории Касперского", установленных на устройствах, путем создания и запуска *задач*. С помощью задач выполняются установка, запуск и остановка программ, проверка файлов, обновление баз и модулей программ, другие действия с программами.

Вы можете создать задачу для программы в Kaspersky Security Center 14.2 Web Console, только если для этой программы установлен плагин управления на сервере Kaspersky Security Center 14.2 Web Console.

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования, включают:

- автоматическая рассылка отчетов;
- загрузку обновлений в хранилище;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

На устройствах выполняются следующие типы задач:

- *Локальные задачи* – это задачи, которые выполняются на конкретном устройстве.

  Локальные задачи могут быть изменены не только администратором средствами Консоли администрирования, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

- *Групповые задачи* – это задачи, которые выполняются на всех устройствах указанной группы.

  Если иное не указано в свойствах задачи, групповая задача также распространяется на подгруппы указанной группы. Групповые задачи также действуют (опционально) и на устройства, подключенные к подчиненным и виртуальным Серверам администрирования, размещенным в этой группе и подгруппах.

- *Глобальные задачи* – это задачи, которые выполняются на выбранных устройствах, независимо от их вхождения в группы администрирования.

Для каждой программы вы можете создавать любое количество групповых задач, глобальных задач и локальных задач.

Вы можете вносить изменения в параметры задач, наблюдать за выполнением задач, копировать, экспортировать и импортировать, а также удалять задачи.

Запуск задач на устройстве выполняется только в том случае, если запущена программа, для которой созданы эти задачи.

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

Не используйте в параметрах задач конфиденциальные данные. Например, старайтесь не указывать пароль доменного администратора.

## См. также:

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

## Область задачи

*Область задачи* (см. стр. 1109) – это подмножество устройств, на которых выполняется задача. Существуют следующие типы областей задачи:

- Область *локальной задачи* – само устройство.
- Область *задачи Сервера администрирования* – Сервер администрирования.
- Область *групповой задачи* – перечень устройств, входящих в группу.

При создании *глобальной задачи* можно использовать следующие методы определения ее области:

- Вручную указать требуемые устройства.

  В качестве адреса устройства вы можете использовать IP-адрес (или IP-интервал), NetBIOS- или DNS-имя.

- Импортировать список устройств из файла формата TXT, содержащего перечень адресов добавляемых устройств (каждый адрес должен располагаться в отдельной строке).

Если список устройств импортируется из файла или формируется вручную, а устройства идентифицируются по имени, то в список могут быть добавлены только те устройства, информация о которых уже занесена в базу данных Сервера администрирования. Данные должны быть занесены в базу при подключении этих устройств или в результате обнаружения устройств.

- Указать выборку устройств.

  С течением времени область действия задачи изменяется по мере того, как изменяется множество устройств, входящих в выборку. Выборка устройств может быть построена на основе атрибутов устройств, в том числе на основе установленного на устройстве программного обеспечения, а также на основе присвоенных устройству тегов. Выборка устройств является наиболее гибким способом задания области действия задачи.

  Запуск по расписанию задач для выборок устройств всегда осуществляет Сервер администрирования. Такие задачи не запустятся на устройствах, не имеющих связи с Сервером администрирования. Задачи, область действия которых задается другим способом, запускаются непосредственно на устройствах и не зависят от наличия связи устройства с Сервером администрирования.

Задачи будут запускаться не по локальному времени устройства, а по локальному времени Сервера администрирования. Задачи, область действия которых задается другим способом, запускаются по локальному времени устройства.

### См. также:

Задачи.....1108

## Создание задачи

► *Чтобы создать задачу:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.
3. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

### См. также:

Задачи.....1108

Общие параметры задач.....1112

Сценарий: Развертывание программ "Лаборатории Касперского".....1035

Сценарий: Мониторинг и отчеты.....1360

Сценарий: Настройка защиты сети.....400

## Запуск задачи вручную

Программа запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время.

► *Чтобы запустить задачу вручную:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. В отобразившемся списке задач установите флажок напротив задачи, которую вы хотите запустить.
3. Нажмите на кнопку **Запустить**.

Задача будет запущена. Вы можете проверить статус задачи в графе **Статус** или нажав на кнопку **Результат**.

### См. также:


О задачах ..... 1109

Создание задачи ..... 1111

Общие параметры задач ..... 1112

Сценарий: Настройка защиты сети ..... 400


## Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center.

► *Чтобы просмотреть список задач,*

В главном окне программы перейдите к закладке **Устройства** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которыми они относятся. Например, задача Удаленная деинсталляция программы относится к Серверу администрирования, а задача Поиск уязвимостей и требуемых обновлений относится к Агенту администрирования.

► *Чтобы просмотреть свойства задачи,*

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными закладками (см. стр. 1112). Например, **Тип задачи** отображается на закладке **Общие**, а расписание задачи на закладке **Расписание**.

### См. также:


Задачи ..... 1108

Сценарий: Настройка защиты сети ..... 400

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516


## Общие параметры задач

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

**Параметры, заданные при создании задачи**

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

    В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

  - **Запрашивать у пользователя**

    На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

    По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

    После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

  - **Принудительно закрывать программы в заблокированных сеансах**

    Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

    Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:
  - **Параметры Запуск по расписанию:**
    - **Каждый N час**

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

    - **Каждый N день**

      Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

      По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    - **Каждую N неделю**

      Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

    - **N минут**

      Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

      По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

    - **Ежедневно (не поддерживает переход на летнее время)**

      Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

      Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

      По умолчанию задача запускается каждый день в текущее системное время.

    - **Еженедельно**

      Задача запускается каждую неделю в указанный день и в указанное время.

    - **По дням недели**

      Задача выполняется регулярно, в указанные дни недели, в указанное время.

      По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При загрузке обновлений в хранилище**

  Эта задача запускается после загрузки обновлений в хранилище. Например, вам может понадобиться это расписание для задачи поиска уязвимостей и требуемых обновлений.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и

**Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования.**

    В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

    Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

  - **Задать адреса устройств вручную или импортировать из списка**

    Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

    Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

  - **Назначить задачу выборке устройств**

    Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

    Например, вы можете использовать этот параметр, чтобы запустить задачу на

устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

  Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.

- Параметры учетной записи:
  - **Учетная запись по умолчанию.**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись:**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль**

    Пароль учетной записи, от имени которой будет запускаться задача.

**Параметры, заданные после создания задачи**

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:
  - **Распределить по подгруппам**
  - **Распространять на подчиненные и виртуальные Серверы администрирования**
- Дополнительные параметры расписания:
  - **Активировать устройство перед запуском задачи функцией Wake On LAN за (мин)**

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройство после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройство после выполнения задачи**

Например, вы можете включить этот параметр для задачи установки обновлений, которая устанавливает обновления на клиентские устройства каждую пятницу после рабочего времени, а затем выключает эти устройства на выходные.

По умолчанию параметр выключен.

- **Остановить, если задача выполняется дольше (мин)**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:
  - Блок **Сохранять информацию о результатах**:
    - **На Сервере администрирования в течение (сут)**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

- **В журнале событий ОС на клиентском устройстве**

События программы, связанные с выполнением задачи, хранятся локально в журнале событий Windows каждого клиентского устройства.

По умолчанию параметр выключен.

- **В журнале событий ОС на Сервере администрирования**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в журнале событий Windows операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранять все события**

Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события о ходе выполнения задачи**

Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения**

Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **Выборка устройств**

Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

### См. также:

Сценарий: Развертывание программ "Лаборатории Касперского" .....1035

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Экспорт задачи

Kaspersky Security Center позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи (см. стр. 1120) как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

► *Чтобы экспортировать задачу:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспортировать** будет неактивна. Задачи Сервера администрирования и локальные задачи также недоступны для экспорта.
3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла задачи и путь. Нажмите на кнопку **Сохранить**.

Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл задачи автоматически сохраняется в папку **Загрузки**.

## Импорт задачи

Kaspersky Security Center позволяет импортировать задачу из файла KLT. Файл KLT содержит экспортированную задачу (см. стр. 1119) и ее параметры.

► *Чтобы импортировать задачу:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл задачи, которую вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу KLT задачи и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл задачи.

   Начнется обработка задачи.
5. После того как задача будет успешно обработана, выберите устройства, которым вы хотите назначить задачу. Для этого выберите один из следующих параметров:
   - **Назначить задачу группе администрирования**

     В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования. Можно указать одну из существующих групп или создать новую группу.

     Например, вы можете использовать этот параметр, чтобы запустить задачу отправки сообщения пользователям, если сообщение предназначено для устройств из определенной группы администрирования.
   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать NetBIOS-имена, DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.
   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.
6. Укажите область действия задачи.
7. Нажмите на кнопку **Готово**, чтобы завершить задачу импорта.

Появится уведомление с результатами импорта. Если задача успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств задачи.

После успешного импорта задача отображается в списке задач. Параметры задачи и расписание также импортируются. Задача будет запущена в соответствии с расписанием.

Если имя новой импортированной задачи идентично имени существующей задачи, имя импортированной задачи расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

## Запуск мастера изменения паролей задач

Для не-локальной задачи можно указать учетную запись, с правами которой будет запускаться задача. Учетную запись можно указать во время создания задачи или в свойствах существующей задачи. Если указанная учетная запись используется в соответствии с правилами безопасности, установленными в организации, эти правила могут требовать периодического изменения пароля учетной записи. После истечения срока действия пароля учетной записи и задания нового пароля, задача не будет запускаться до тех пор, пока вы не укажете новый действующий пароль в свойствах задачи.

Мастер изменения паролей задач позволяет автоматически заменить старый пароль на новый во всех задачах, в которых указана учетная запись. Вы также можете изменить пароль вручную в свойствах каждой задачи.

► *Чтобы запустить мастер изменения паролей задач:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

### См. также:



### В этом разделе



### Шаг 1. Выбор учетных данных

Укажите новые учетные данные, действующие в вашей системе (например, в Active Directory). При переходе на следующий шаг мастера, Kaspersky Security Center проверяет, совпадает ли имя указанной учетной записи с именем учетной записи в свойствах каждой не-локальной задачи. Если имена учетных записей совпадают, пароль в свойствах задачи автоматически меняется на новый.

Чтобы указать новую учетную запись, выберите один из вариантов:

- **Использовать текущую учетную запись**

  Мастер использует имя учетной записи, под которой вы в настоящее время вошли в Kaspersky Security Center 14.2 Web Console. Вручную укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

- **Указать другую учетную запись**

  Укажите имя учетной записи, под которой должны запускаться задачи. Укажите пароль учетной записи в поле **Актуальный пароль для использования в задачах**.

При заполнении поля **Предыдущий пароль (необязательно; если вы хотите заменить его на текущий)** Kaspersky Security Center заменит пароль только для тех задач, для которых совпадают значения имени и старого пароля. Замена выполняется автоматически. Во всех остальных случаях необходимо выбрать действие, выполняемое на следующем шаге мастера.

## См. также:



## Шаг 2. Выбор выполняемого действия

Если на первом шаге мастера вы не указали предыдущий пароль или если указанный старый пароль не соответствует паролям, которые указаны в свойствах задач, необходимо выбрать действие, выполняемое с этими задачами.

► *Чтобы выбрать действие с задачей:*

1. Установите флажок около задачи, с которой вы хотите выполнить действие.
2. Выполните одно из следующих действий:
   - Чтобы удалить пароль в свойствах задачи, нажмите **Удалить учетные данные**.

     Задача переключена на запуск под учетной записью по умолчанию.
   - Чтобы заменить пароль на новый, нажмите **Принудительно изменить пароль, даже если старый пароль неверен или не указан**.
   - Чтобы отменить изменение пароля, нажмите **Действие не выбрано**.

   Выбранные действия применяются после перехода к следующему шагу мастера.

## См. также:



## Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

## См. также:

kaspersky

# Управление клиентскими устройствами

В этом разделе описано, как управлять устройствами в группах администрирования.

## В этом разделе



## См. также:



## Параметры управляемого устройства

► *Чтобы просмотреть параметры управляемого устройства:*

1. Выберите **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

В верхней части окна свойств отображаются следующие закладки, на которых представлены основные группы параметров:

- **Общие**
- **Программы**
- **Активные политики и профили политик**
- **Задачи**
- **События**
- **Инциденты**

- **Теги**
- **Дополнительно**

## См. также:

Настройка общих параметров Сервера администрирования .....685

## Создание групп администрирования

Сразу после установки Kaspersky Security Center в иерархии групп администрирования присутствует только одна группа администрирования – **Управляемые устройства**. При создании иерархии групп администрирования в состав папки **Управляемые устройства** можно включать устройства и виртуальные машины и добавлять вложенные группы. (см. рисунок ниже).

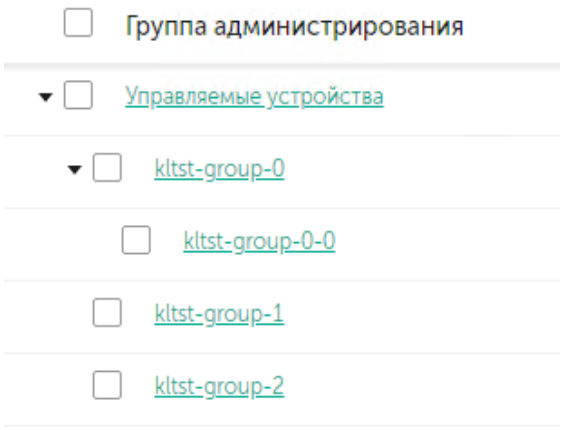



Figure 15. Просмотр иерархии групп администрирования

► *Чтобы создать группу администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.

В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Программа позволяет создавать структуру групп администрирования на основе структуры Active Directory или структуры доменной сети. Также вы можете создавать структуру групп из текстового файла.

► *Чтобы создать структуру групп администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

kaspersky

## Добавление устройств в состав группы администрирования вручную

Вы можете перемещать устройства в группы администрирования автоматически, создавая правила перемещения устройств, или вручную, перемещая устройства из одной группы администрирования в другую, или добавляя устройства в выбранную группу администрирования. В этом разделе описано, как вручную добавить устройства в группу администрирования.

► *Чтобы вручную добавить одно или несколько устройств в состав выбранной группы администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь:** `<current path>` над списком.
3. В открывшемся окне выберите группу администрирования, в которую требуется добавить устройства.
4. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.
5. Составьте список устройств, которые вы хотите добавить в группу администрирования.

   > В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

   Выберите, как вы хотите добавить устройства в список:

   - Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
     - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
     - Укажите IP-адреса устройств или IP-диапазон.
     - Укажите NetBIOS-имя устройства или DNS-имя.

       > Поле с именем устройства не должно содержать пробелы, а также следующие запрещенные символы: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %.

   - Нажмите на кнопку **Импортировать устройства из файла**, чтобы импортировать список устройств из файла формата TXT. Каждый адрес устройства (или имя устройства) должен располагаться в отдельной строке.

     > Файл не должен содержать пробелы, а также следующие запрещенные символы: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %.
6. Просмотрите список устройств, которые будут добавлены в группу администрирования. Вы можете редактировать список, добавляя или удаляя устройства.
7. После того как вы убедитесь, что в списке нет ошибок, нажмите на кнопку **Далее**.

Мастер обрабатывает список устройств и отображает результат. После завершения работы мастера выбранные устройства включаются в состав группы администрирования и отображаются в списке устройств под именами, установленными для них Сервером администрирования.

См. также:



## Перемещение устройств в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

► *Чтобы переместить одно или несколько устройств в состав выбранной группы администрирования:*

1. Откройте группу администрирования, в которую вы хотите переместить устройства. Для этого выполните одно из следующих действий:
   - Чтобы открыть группу администрирования, в главном меню перейдите в раздел **Устройства** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** и в открывшейся слева панели выберите группу администрирования.
   - Чтобы открыть группу **Нераспределенные устройства**, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Установите флажки рядом с устройствами, которые требуется переместить в другую группу.
3. Нажмите на кнопку **Переместить в группу**.
4. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства.
5. Нажмите на кнопку **Переместить**.

Выбранные устройства перемещаются в выбранную группу администрирования.

## Создание правил перемещения устройств

Можно настроить правила перемещения устройств (см. стр. 445), в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне программы перейдите в раздел **Устройства** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне укажите следующие данные на закладке **Общие**:
   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).
   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - Запустить однократно на каждом устройстве.

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - Запустить однократно на каждом устройстве, а затем при каждой установке Агента администрирования.

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - Применять правило постоянно.

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Включить правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

4. На закладке **Условия правила** укажите (см. стр. 1129) хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.
5. Нажмите на кнопку **ОК**.

Будет создано правило перемещения. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет. Чтобы повысить или понизить приоритет правила перемещения, с помощью мыши переместите правило вверх или вниз по списку соответственно.

Если атрибуты устройства удовлетворяют сразу нескольким правилам, то устройство будет перемещено в целевую группу того правила, которое имеет больший приоритет (стоит в списке правил выше).

## См. также:

Добавление устройств в состав группы администрирования вручную .....1125

Сценарий: Обнаружение устройств в сети.....324

## Копирование правил перемещения устройств

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:
   - В главном окне программы перейдите в раздел **Устройства** → **Правила перемещения**.
   - В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → Развертывание и назначение → **Правила перемещения**.

   Отобразится список правил перемещения устройств.
2. Установите флажок напротив правила, которое требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне при необходимости измените данные на закладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:
   - **Имя правила**

     Укажите имя нового правила активации.

     Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).
   - **Группа администрирования**

     Выберите группу администрирования, в которую будут автоматически перемещаться устройства.
   - **Применить правило**

     Вы можете выбрать один из следующих вариантов:
     - Запустить однократно на каждом устройстве.

       Правило применяется однократно для каждого устройства, соответствующего указанным критериям.
     - Запустить однократно на каждом устройстве, а затем при каждой установке Агента администрирования.

       Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.
     - Применять правило постоянно.

       Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).
   - **Перемещать только устройства, которые не входят ни в одну группу администрирования**

     Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

     Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.
   - **Включить правило**

     Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

     Если этот параметр выключен, правило создается, но оно не включено. Правило не

будет работать до тех пор, пока вы не включите этот параметр.

5. При необходимости на закладке **Условия правила** укажите (см. стр. 1129) критерии для устройств, которые требуется переместить автоматически.
6. Нажмите на кнопку **ОК**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

## См. также:

Сценарий: Обнаружение устройств в сети.....324

## Условия для правила перемещения устройств

При создании (см. стр. 1126) или же копировании (см. стр. 1127) правила перемещения клиентских устройств в группы администрирования, на закладке **Условия правила** вы задаете условия перемещения устройств (см. стр. 445). Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Управляемые программы, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.
- Информация об организационной единице Active Directory (OU) с клиентскими устройствами.
- Информация об облачном сегменте с клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

### Закладка Теги

На этой закладке можно настроить поиск устройств по ключевым словам (тегам) (см. стр. 1159), которые были добавлены ранее в описания управляемых устройств. Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

- **Применять к устройствам без выбранных тегов**
- **Применять, если есть хотя бы один из выбранных тегов**

### Закладка Сеть

На этой закладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **Имя устройства в сети Windows**
- **Windows-домен**
- **DNS-имя устройства**

- **DNS-домен**
- **IP-диапазон**
- **IP-адрес подключения к Серверу администрирования**
- **Изменение профиля подключения**
- **Под управлением другого Сервера администрирования**

**Закладка Программы**

На этой закладке можно настроить правило перемещения устройств на основе управляемых программ и операционных систем, установленных на клиентских устройствах:

- **Установлен Агент**
- **Программы**
- **Версия операционной системы**
- **Разрядность операционной системы**
- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.
- **Пользовательский сертификат**
- **Номер сборки операционной системы**
- **Номер выпуска операционной системы**

**Закладка Виртуальные машины**

На этой закладке можно настроить параметры правила перемещения устройств в зависимости от того, являются эти устройства виртуальными машинами или частью инфраструктуры виртуальных рабочих столов (VDI):

- **Является виртуальной машиной**
- **Тип виртуальной машины**
- **Часть Virtual Desktop Infrastructure**

**Закладка Active Directory**

На этой закладке можно указать, что необходимо перемещать устройства, входящие в организационную единицу Active Directory. Также можно переместить устройства из всех дочерних подразделений указанного подразделения Active Directory:

- **Устройство находится в подразделении Active Directory**
- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию параметр выключен.
- **Перемещать устройства из дочерних объектов в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**

- **Удалять подгруппы, отсутствующие в Active Directory**
- **Устройство является членом группы Active Directory**

**Закладка Облачные сегменты**

На этой закладке можно указать, что необходимо перемещать устройства, которые относятся к определенным облачным сегментам:

- **Устройство находится в облачном сегменте**
- **Включать дочерние объекты**
- **Перемещать устройства из вложенных объектов в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, для которых нет соответствия в облачных сегментах**
- **Устройство обнаружено с помощью API**

  В раскрывающемся списке можно выбрать, обнаруживается ли устройство средствами API:

  - **AWS**. Устройство обнаружено с использованием AWS API, то есть устройство находится в облачном окружении AWS.
  - **Azure**. Устройство обнаружено с использованием Azure API, то есть устройство находится в облачном окружении Azure.
  - **Google Cloud.** Устройство обнаружено с использованием Google API, то есть устройство находится в облачном окружении Google.
  - **Нет**. Устройство не обнаруживается с помощью AWS, Azure или Google API, то есть оно либо находится вне облачного окружения, либо находится в облачном окружении, но недоступно для поиска с помощью API.
  - **Не задано**. Условие не применяется.

## Просмотр и настройка действий, когда устройство неактивно

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

► *Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. Выберите имя требуемой группы администрирования.

   Откроется окно свойств группы администрирования.
3. В окне свойств перейдите в раздел **Параметры**.
4. В разделе **Наследование** включите или выключите следующие параметры:

   - **Наследовать из родительской группы**

     Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств** недоступны для изменения.

     Этот параметр доступен только для группы администрирования, у которой есть

родительская группа администрирования.

По умолчанию параметр включен.

- **Обеспечить принудительное наследование параметров для дочерних групп**

  Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

  По умолчанию параметр выключен.

5. В разделе **Активность устройств** включите или выключите следующие параметры:

   - **Уведомлять администратора, если устройство неактивно больше (сут)**

     Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

     По умолчанию параметр включен.

6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

## О статусах устройства

Kaspersky Security Center присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *ОК* или *ОК / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

*Таблица 87. Условия присвоения статусов устройству*

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Не установлена программа безопасности | Агент администрирования установлен на устройстве, но не установлена программа безопасности. | • Переключатель включен.<br>• Переключатель выключен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Найдено много вирусов | В результате работы задач поиска вирусов, например, задачи *Поиск вредоносного ПО*, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение. | Более 0. |
| Уровень постоянной защиты отличается от уровня, установленного администратором | Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства. | • Остановлена.<br>• Приостановлена.<br>• Выполняется. |
| Давно не выполнялся поиск вредоносного ПО | Устройство видимо в сети и на устройстве установлена программа безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее. | Более 1 дня. |
| Базы устарели | Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее. | Более 1 дня. |
| Давно не подключались | Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. | Более 1 дня. |
| Обнаружены активные угрозы | Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение. | Более чем 0 штук. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Требуется перезагрузка | Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин. | Более чем 0 минут. |
| Установлены несовместимые программы | Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы. | • Переключатель выключен.<br>• Переключатель включен. |
| Обнаружены уязвимости в программах | Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в программах с заданным уровнем критичности. | • Предельный.<br>• Высокий.<br>• Средний.<br>• Игнорировать, если нельзя закрыть уязвимость.<br>• Игнорировать, если обновление назначено к установке. |
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истек. | • Переключатель выключен.<br>• Переключатель включен. |
| Срок действия лицензии истекает | Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней. | Более чем 0 дней. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Давно не выполнялась проверка обновлений Центра обновления Windows | Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени. | Более 1 дня. |
| Недопустимый статус шифрования | Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению. | • Не соответствует политике из-за отказа пользователя (только для внешних устройств).<br>• Не соответствует политике из-за ошибки.<br>• В процессе применения политики – требуется перезагрузка.<br>• Не задана политика шифрования.<br>• Не поддерживается.<br>• В процессе применения политики. |
| Параметры мобильного устройства не соответствуют политике | Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия. | • Переключатель выключен.<br>• Переключатель включен. |
| Есть необработанные инциденты | На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. | • Переключатель выключен.<br>• Переключатель включен. |
| Статус устройства определен программой | Статус устройства определяется управляемой программой. | • Переключатель выключен.<br>• Переключатель включен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| На устройстве заканчивается дисковое пространство | Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению. | Более чем 0 МБ. |
| Устройство стало неуправляемым | Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования. | • Переключатель выключен.<br>• Переключатель включен. |
| Защита выключена | Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени. | Более чем 0 минут. |
| Программа безопасности не запущена | Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена. | • Переключатель выключен.<br>• Переключатель включен. |

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *ОК*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

kaspersky

См. также:

Настройка переключения статусов устройств .....1449

## Настройка переключения статусов устройств

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*.

► *Чтобы изменить статус устройства на* Критический*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Критический"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

► *Чтобы изменить статус устройства на* Предупреждение*:*

1. Откройте окно свойств одним из следующих способов:
   - В папке **Политики** в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
   - В контекстном меню группы администрирования выберите пункт **Свойства**.
2. В окне свойств группы администрирования выберите раздел **Статус устройства**.
3. В блоке **Установить статус "Предупреждение"** установите флажок для условия из списка.
4. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
5. Нажмите на кнопку **ОК**.

Разным значениям одного условия могут соответствовать разные статусы. Например, при соблюдении условия **Базы устарели** со значением `Более 7 дней` клиентскому устройству присваивается статус *Предупреждение*, а со значением `Более 14 дней` – статус *Критический*.

В таблице приведены условия для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения

*Таблица 88. Условия присвоения статусов устройству*

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Не установлена программа безопасности | Агент администрирования установлен на устройстве, но не установлена программа безопасности. | • Флажок установлен.<br>• Флажок снят. |
| Обнаружено много вирусов | В результате работы задач поиска вирусов, например, задачи Поиск вредоносного ПО, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение. | Более 0 |
| Уровень постоянной защиты отличается от уровня, установленного администратором | Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства. | • Остановлена.<br>• Приостановлена.<br>• Выполняется. |
| Давно не выполнялся поиск вредоносного ПО | Устройство видимо в сети и на устройстве установлена программа безопасности, но задача поиска вирусов не выполнялась больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее. | Более 1 дня |
| Базы устарели | Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее. | Более 1 дня |
| Давно не подключались | Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. | Более 1 дня |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Обнаружены активные угрозы | Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение. | Более чем 0 штук |
| Требуется перезагрузка | Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин. | Более чем 0 минут |
| Установлены несовместимые программы | Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы. | • Флажок снят.<br>• Флажок установлен. |
| Обнаружены уязвимости в программах | Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи Поиск уязвимостей и требуемых обновлений на устройстве обнаружены уязвимости в программах с заданным уровнем критичности. | • Предельный.<br>• Высокий.<br>• Средний.<br>• Игнорировать, если нельзя закрыть уязвимость.<br>• Игнорировать, если обновление назначено к установке. |
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истек. | • Флажок снят.<br>• Флажок установлен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней. | Более чем 0 дней |
| Давно не выполнялась проверка обновлений Центра обновления Windows | Не выполнялась задача Синхронизация обновлений Windows Update больше указанного времени. | Более 1 дня |
| Указанный статус шифрования | Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению. | • Не соответствует политике из-за отказа пользователя (только для внешних устройств).<br>• Не соответствует политике из-за ошибки.<br>• В процессе применения политики – требуется перезагрузка.<br>• Не задана политика шифрования.<br>• Не поддерживается.<br>• В процессе применения политики. |
| Параметры мобильного устройства не соответствуют политике | Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия. | • Флажок снят.<br>• Флажок установлен. |
| Есть необработанные инциденты | На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. | • Флажок снят.<br>• Флажок установлен. |
| Статус устройства определен программой | Статус устройства определяется управляемой программой. | • Флажок снят.<br>• Флажок установлен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| На устройстве заканчивается дисковое пространство | Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению. | Более чем 0 МБ |
| Устройство стало неуправляемым | Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования. | • Флажок снят.<br>• Флажок установлен. |
| Защита выключена | Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени. | Более чем 0 минут |
| Программа безопасности не запущена | Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена. | • Флажок снят.<br>• Флажок установлен. |

См. также:

Настройка общих параметров Сервера администрирования .....685

## Удаленное подключение к рабочему столу клиентского устройства

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

После подключения к устройству администратор получает полный доступ к информации на этом устройстве и может управлять программами, установленными на нем.

Удаленное подключение должно быть разрешено в параметрах операционной системы целевого управляемого устройства. Например, в Windows 10 этот параметр называется **Разрешить подключения удаленного помощника к этому компьютеру** (его можно найти **Панель управления** → **Система и безопасность** → **Система** → **Настройка удаленного доступа**). Если у вас есть лицензия на Системное администрирование, вы можете принудительно включить этот параметр, когда установлено соединение с управляемым устройством. Если у вас нет лицензии, включите этот параметр локально на целевом управляемом устройстве. Если этот параметр выключен, удаленное подключение невозможно.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт брандмауэром.
- Стандартный компонент Microsoft Windows "Подключение к удаленному рабочему столу". Подключение к удаленному рабочему столу выполняется с помощью штатной утилиты Windows mstsc.exe в соответствии с параметрами работы этой утилиты.

  Подключение к существующему сеансу удаленного рабочего стола пользователя осуществляется без уведомления пользователя. После подключения администратора к сеансу пользователь устройства будет отключен от сеанса без предварительного уведомления.

► *Чтобы удалено подключиться к рабочему столу клиентского устройства:*

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования** → **Порты подключения**.
3. Убедитесь, что параметр **Открыть порт для Kaspersky Security Center Web Console** включен.
4. В Kaspersky Security Center 14.2 Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.
7. Установите флажок напротив устройства, к которому вы хотите получить доступ.

8. Нажмите на кнопку **Удаленный рабочий стол (только Windows)**.

   Откроется окно Удаленный рабочий стол (только Windows).

9. Включите параметр **Разрешить подключение к удаленному рабочему столу на управляемом устройстве**. В этом случае соединение будет установлено, даже если удаленные подключения в настоящее время запрещены в параметрах операционной системы на управляемом устройстве.

   > Этот параметр доступен только при наличии лицензии на Системное администрирование.

10. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel.
11. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

    > Объект BLOB действителен в течение 3 минут. Если срок его действия истек, снова откройте окно Удаленный рабочий стол (только Windows), чтобы сгенерировать новый объект BLOB.

12. Запустите утилиту klsctunnel.

    Откроется окно утилиты.

13. Вставьте скопированный текст в текстовое поле.
14. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
15. Нажмите на кнопку **Открыть порт**.

    Откроется окно входа в систему подключения к удаленному рабочему столу.

16. Укажите учетные данные учетной записи, под которой вы в настоящий момент входите Kaspersky Security Center 14.2 Web Console.
17. Нажмите на кнопку **Подключиться**.

После подключения к клиентскому устройству рабочий стол клиентского устройства доступен в окне удаленного подключения Microsoft Windows.

## Подключение к устройствам с помощью совместного доступа к рабочему столу Windows

Администратор может получить удаленный доступ к рабочему столу клиентского устройства с помощью Агента администрирования, установленного на устройстве. Удаленное подключение к клиентскому устройству с помощью Агента администрирования возможно и в том случае, если TCP- и UDP-порты клиентского устройства закрыты для доступа.

Администратор может подключиться к существующему сеансу на клиентском устройстве без отключения пользователя, работающего в этом сеансе. В этом случае у администратора и пользователя сеанса на устройстве есть совместный доступ к рабочему столу.

Чтобы установить удаленное соединение с устройством, у вас должно быть две утилиты:

- Утилита klsctunnel "Лаборатории Касперского". Эта утилита должна храниться на рабочей станции администратора. Вы используете эту утилиту для туннелирования соединения между клиентским устройством и Сервером администрирования.

  Kaspersky Security Center позволяет туннелировать TCP-соединения от Консоли администрирования через Сервер администрирования и далее через Агент администрирования к заданному порту на управляемом устройстве. Туннелирование используется для подключения клиентского приложения, находящегося на устройстве с установленной Консолью администрирования, к TCP-порту на управляемом устройстве, если прямое соединение устройства с Консолью администрирования с устройством невозможно.

  Туннелирование соединения удаленного клиентского устройства с Сервером администрирования необходимо, если на устройстве недоступен порт для соединения с Сервером администрирования. Порт на устройстве может быть недоступен в следующих случаях:

  - Удаленное устройство подключено к локальной сети, в которой используется механизм NAT.
  - Удаленное устройство входит в локальную сеть Сервера администрирования, но его порт закрыт брандмауэром.

- Совместный доступ к рабочему столу Windows. При подключении к существующему сеансу удаленного рабочего стола пользователь этого сеанса на устройстве получит запрос от администратора на подключение. Информация о процессе удаленной работы с устройством и результатах этой работы не сохраняется в отчетах Kaspersky Security Center.

  Администратор может настроить аудит действий на удаленном клиентском устройстве. В ходе аудита программа сохраняет информацию о файлах на устройстве, которые открывал и/или изменял администратор (см. стр. 721).

Для подключения к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows требуется выполнение следующих условий:

- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- На рабочем месте администратора установлена операционная система Microsoft Windows Vista или более поздняя версия. Тип операционной системы устройства, на котором установлен Сервер администрирования, не является ограничением для подключения с помощью совместного доступа к рабочему столу Windows.

  Чтобы проверить, включена ли функция совместного доступа к рабочему столу Windows в вашей версии Windows, убедитесь, что ключ CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} включен в реестр Windows .
- На клиентском устройстве установлена операционная система Microsoft Windows Vista или более поздняя версия.
- Kaspersky Security Center использует лицензию на Системное администрирование.

► *Чтобы подключиться к рабочему столу клиентского устройства с помощью совместного доступа к рабочему столу Windows:*

1. В Консоли администрирования на основе MMC в контекстном меню политики Сервера администрирования выберите пункт **Свойства**.
2. В открывшемся окне свойств Сервера администрирования перейдите в раздел **Параметры подключения к Серверу администрирования → Порты подключения**.
3. Убедитесь, что параметр **Открыть порт для Kaspersky Security Center Web Console** включен.

4. В Kaspersky Security Center 14.2 Web Console перейдите в раздел **Устройства** → **Управляемые устройства**.
5. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
6. В открывшейся панели слева выберите группу администрирования, содержащую устройство, к которому вы хотите получить доступ.
7. Установите флажок напротив устройства, к которому вы хотите получить доступ.
8. Нажмите на кнопку **Совместный доступ к рабочему столу Windows**.

   Открывается мастер совместного доступа к рабочему столу Windows.
9. Нажмите на кнопку **Загрузить**, чтобы загрузить утилиту klsctunnel, и дождитесь завершения процесса загрузки.

   Если у вас уже есть утилита klsctunnel, пропустите этот шаг.
10. Нажмите на кнопку **Далее**.
11. Выберите сеанс на устройстве, к которому вы хотите подключиться, а затем нажмите на кнопку **Далее**.
12. На целевом устройстве в открывшемся окне пользователь должен разрешить сеанс совместного доступа к рабочему столу. Иначе сеанс невозможен.

    После того как пользователь подтвердит сеанс совместного доступа к рабочему столу, мастер откроет следующий шаг.
13. Нажмите на кнопку **Копировать в буфер обмена**, чтобы скопировать текст из текстового поля. Этот текст представляет собой двоичный объект данных (BLOB), который содержит параметры, необходимые для установления соединения между Сервером администрирования и управляемым устройством.

    > Объект BLOB действителен в течение 3 минут. Если срок его действия истек, сгенерируйте объект BLOB.
14. Запустите утилиту klsctunnel.

    Откроется окно утилиты.
15. Вставьте скопированный текст в текстовое поле.
16. Если вы используете прокси-сервер, установите флажок **Использовать прокси-сервер**, а затем укажите параметры подключения к прокси-серверу.
17. Нажмите на кнопку **Открыть порт**.

Совместный доступ к рабочему столу запускается в новом окне. Если вы хотите взаимодействовать с устройством, нажмите на значок Меню (  ) в верхнем левом углу окна и выберите **Интерактивный режим**.

## См. также:


Варианты лицензирования Kaspersky Security Center ..... 353

Порты, используемые Kaspersky Security Center ..... 98

kaspersky

## Выборки устройств

*Выборки устройств* – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Kaspersky Security Center предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом Критический**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки нельзя удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленной программы, то в выборку устройств попадут только те устройства, на которых одновременно установлена указанная программа и их IP-адреса входят в указанный диапазон.

### В этом разделе



### Просмотр списка устройств из выборки устройств

Kaspersky Security Center позволяет просматривать список устройств из выборки устройств.

► *Чтобы просмотреть список устройств из выборки устройств:*

1. В главном окне программы перейдите в раздел **Устройства** → **Выборки устройств** или в раздел **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:
   - Нажмите на значок параметров ( ) и выберите столбцы для отображения в таблице.
   - Нажмите на значок фильтрации ( ), укажите и примените критерий фильтрации в открывшемся меню.

Отобразится отфильтрованная таблица устройств.

Вы можете выбрать одно или несколько устройств в выборке устройств и нажать на кнопку **Новая задача**, чтобы создать задачу (см. стр. 1108), которая будет применена к этим устройствам.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

## Создание выборки устройств

► *Чтобы создать выборку устройств:*

1. В главном окне программы перейдите в раздел **Устройства** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.

3. Введите имя новой выборки.

4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:

   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.
   - **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.
   - **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

   Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.

5. Нажмите на кнопку **Добавить**.

6. В открывшемся окне укажите условия (см. стр. 1147), которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **ОК**.

7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

## Настройка выборки устройств

► *Чтобы настроить параметры выборки устройств:*

1. В главном окне программы перейдите в раздел **Устройства** → **Выборки устройств**.

   Отобразится страница со списком выборок устройств.

2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.

3. На закладке **Общие** перейдите по ссылке **Новое условие**.

4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.

5. Нажмите на кнопку **Сохранить**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

**Инвертировать условие выборки**

Если этот параметр включен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию параметр выключен.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя), IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Отображаются все устройства, входящие в указанный Windows-домен.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Описание** допустимо использовать следующие символы:

  - Внутри одного слова:
    - *****. Заменяет любую строку длиной 0 и более символов.

    **Пример**:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

    **Пример**:

    Для описания слов **Окно** или **Окна** можно использовать строку **Окн?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

  - Для связи нескольких слов:
    - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

    **Пример**:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный**

можно использовать строку **Подчиненный Виртуальный**.

- **+**. При написании перед словом обозначает обязательное наличие слова в тексте.

**Пример**:

Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

**Пример**:

Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

**Пример**:

Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство находится в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы Active Directory.

  По умолчанию параметр выключен.

- **Это устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

- **Да**. В выборку будут включены устройства, являющиеся точками распространения.
- **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
- **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. В выборку будут включаться устройства, на которых установлен флажок **Не разрывать соединение с Сервером администрирования**.
  - **Выключен**. В выборку будут включаться устройства, на которых флажок **Не разрывать соединение с Сервером администрирования** снят.
  - **Значение не выбрано**. Критерий не применяется.

- **Переключение профиля подключения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- **Последнее подключение к Серверу администрирования**

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Новые устройства, обнаруженные при опросе сети**

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- **Устройство в сети**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. Программа включает в выборку устройства, которые видимы в сети в

настоящий момент.

- **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
- **Значение не выбрано**. Критерий не применяется.

В разделе **Облачные сегменты** можно настроить критерии включения устройств в выборку в соответствии с облачными сегментами:

- **Устройство находится в облачном сегменте**
- **Устройство обнаружено с помощью API**

Статус устройства

В разделе **Статус устройства** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемой программы:

- **Статус устройства**

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *ОК*, *Критический* или *Предупреждение*.

- **Статус постоянной защиты**

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- **Описание статуса устройства**

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *ОК, Критический* или *Предупреждение*.

В разделе **Статусы компонентов управляемых программ** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых программ:

- **Статус защиты данных от утечек**

  Поиск устройств по статусу защиты данных от утечек (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

- **Статус защиты для серверов совместной работы**

Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, Сбой).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых программ** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемой программой. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких программ, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы:

- **Тип платформы**

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Разрядность операционной системы**

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64**, **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- **Номер сборки операционной системы**

Этот параметр применим только для операционных систем Windows.

Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- **Номер выпуска операционной системы**

Этот параметр применим только для операционных систем Windows.

Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- **Является виртуальной машиной**
- **Тип виртуальной машины**

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Раскрывающийся список доступен, если в раскрывающемся списке **Является виртуальной машиной** указано значение **Да** или **Неважно**.

- **Часть Virtual Desktop Infrastructure**

В разделе **Реестр оборудования** можно настроить критерии включения устройств в выборку по установленному на них оборудованию:

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить сведения об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора.

- **Устройство**

  В раскрывающемся списке можно выбрать тип оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Поставщик**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

  Имя устройства в Windows-сети. Устройство с указанным именем будет включено в выборку.

- **Описание**

  Описание устройства или оборудования. Устройства с описанием, указанным в поле, будут включены в состав выборки.

  Описание устройства в произвольной форме можно ввести в окне свойств устройства. В поле поддерживается полнотекстовый поиск.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**
- **Частота процессора (МГц) до**
- **Количество виртуальных ядер процессора от**
- **Количество виртуальных ядер процессора до**
- **Объем жесткого диска (ГБ), от**
- **Объем жесткого диска (ГБ), до**
- **Объем оперативной памяти (МБ), от**
- **Объем оперативной памяти (МБ), до**

Информация о программах сторонних производителей

В разделе **Реестр программ** можно настроить критерии включения устройств в выборку в зависимости от того, какие программы на них установлены:

- **Название программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки флажка названия полей ввода **Название программы**, **Версия программы** и **Статус программы** меняются на **Имя обновления**, **Версия обновления** и **Статус** соответственно.

  По умолчанию параметр выключен.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

  В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если этот параметр выключен, критерий не применяется.

По умолчанию параметр выключен.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

**WUA переключен на Сервер администрирования**

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **Да**. Если выбран этот вариант, в результаты поиска включаются устройства, которые получают обновления Центра обновления Windows с Сервера администрирования.
- **Нет**. Если выбран этот вариант, в результаты включаются устройства, которые получают обновления Центра обновления Windows из другого источника.

Информация о программах "Лаборатории Касперского"

В разделе **Программа** можно настроить критерии включения устройств в выборку на основании выбранной управляемой программы:

- **Название программы**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

  В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

  Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и

время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

Если флажок снят, то критерий не применяется.

По умолчанию флажок снят.

- **Устройство находится под управлением Kaspersky Security Center 14.2**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

  - **Да**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
  - **Значение не выбрано**. Критерий не применяется.

- **Программа безопасности установлена**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

  - **Да**. Программа включает в выборку устройства, на которых установлена программа безопасности.
  - **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
  - **Значение не выбрано**. Критерий не применяется.

В подразделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Количество записей в базах**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству записей в базе. В полях ввода можно задать нижнее и верхнее значения количества записей.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вредоносного ПО. В полях ввода можно указать интервал, в течение которого поиск вредоносного ПО выполнялся в последний раз.

  По умолчанию параметр выключен.

- **Обнаружены угрозы**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

В подразделе **Шифрование** можно настроить критерии включения устройств в выборку на основе выбранного алгоритма шифрования:

**Алгоритм шифрования**

Стандарт симметричного алгоритма блочного шифрования Advanced Encryption Standard (AES). В раскрывающемся списке вы можете выбрать размер ключа шифрования (56 Бит, 128 Бит, 192 Бит или 256 Бит).

Возможные значения: *AES56*, *AES128*, *AES192* и *AES256*.

Подраздел **Компоненты программы** содержит список компонентов тех программ, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center 14.2 Web Console.

В разделе **Компоненты программы** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранной программе:

- **Статус**
- **Версия**

Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

Теги

В разделе **Теги** можно настроить критерии включения устройств в выборку по ключевым словам (тегам), которые были добавлены ранее в описания управляемых устройств:

**Применить, если есть хотя бы один из выбранных тегов**

Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию параметр выключен.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**

  **Пользователь, уже выполнявший вход в систему**Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

## Экспорт списка устройств из выборки устройств

Kaspersky Security Center позволяет сохранять информацию об этих устройствах из выборки устройств в файл CSV или TXT.

► *Чтобы экспортировать список устройств из выборки устройств в файл:*

1. Откройте таблицу с устройствами (см. стр. 1146) из выборки устройств.
2. Вы можете экспортировать информацию об устройствах из таблицы одним из следующих способов:
   - Экспортировать выбранные устройства.

     Установите флажки рядом с требуемыми устройствами и нажмите на кнопку **Экспортировать строки в файл формата CSV** или **Экспортировать строки в файл формата TXT** в зависимости от формата, который вы хотите экспортировать. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована в файл TXT или CSV.
   - Экспортировать все устройства, отображаемые на текущей странице.

     Нажмите на кнопку **Экспортировать строки в файл формата CSV** или **Экспортировать строки в файл формата TXT**, в зависимости от формата, который вы хотите экспортировать. Вам не нужно выбирать устройства из таблицы. Вся информация об устройствах, отображаемая на текущей странице, будет экспортирована в файл TXT.

Обратите внимание, если вы отфильтровали таблицу устройств, в файл CSV или TXT будут экспортированы только отфильтрованные данные отображаемых столбцов.

## Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

► *Чтобы удалить устройства из групп администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

## Теги устройств

В этом разделе описаны теги устройств, приведены инструкции по их созданию и изменению, а также по назначению тегов устройствам вручную и автоматически.

### См. также:



### В этом разделе



### О тегах устройств

Kaspersky Security Center позволяет назначать *теги* устройствам. Тег представляет собой идентификатор устройства, который можно использовать для группировки, описания, поиска устройств. Назначенные устройствам теги можно использовать при создании выборок устройств (см. стр. 1146), при поиске устройств и при распределении устройств по группам администрирования (см. стр. 81).

Теги могут назначаться устройствам вручную или автоматически. Теги можно назначать вручную, если требуется отметить отдельные устройства. Автоматическое назначение тегов выполняется Kaspersky Security Center в соответствии с заданными правилами назначения тегов.

Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве программам и другим свойствам устройства. Например, если используется гибридная инфраструктура, состоящая из физических устройств, инстансов Amazon EC2 и виртуальных машин Microsoft Azure, можно настроить правило, в соответствии с которым всем виртуальным машинам Microsoft Azure будет назначен тег `[Azure]`. Затем можно использовать этот тег при

создании выборки устройств, чтобы отобрать все виртуальные машины Microsoft Azure и назначить им задачу.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

## См. также:

Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Сценарий: Обнаружение устройств в сети.....1054

Настройка и распространение политик: подход, ориентированный на устройства .....402

## Создание тегов устройств

► *Чтобы создать тег устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите тег.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

## См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Изменение тегов устройств

► *Чтобы переименовать тег устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените тег.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

## См. также:

Сценарий: Обнаружение устройств в сети ..... 1054

## Удаление тегов устройств

► *Чтобы удалить тег устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.
2. В списке выберите теги устройства, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Да**.

Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

Тег, который вы удалили, не удаляется автоматически из правил автоматического назначения тегов. После удаления тега он будет назначен новому устройству только при первом совпадении параметров устройства с условиями правила назначения тегов.
Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству программой или Агентом администрирования. Чтобы удалить тег с вашего устройства, используйте утилиту klscflag (см. стр. 1167).

## См. также:

Сценарий: Обнаружение устройств в сети ..... 1054

## Просмотр устройств, которым назначен тег

► *Чтобы просмотреть устройства с назначенными тегами:*

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.
2. Перейдите по ссылке **Посмотреть устройства** рядом с названием тега, для которого вы хотите посмотреть список назначенных устройств.

   Если ссылка **Посмотреть устройства** не отображается рядом с названием тега, этот тег не назначен ни одному из устройств.

В списке устройств отображаются только устройства, которым назначены теги.

Чтобы вернуться к списку тегов устройства, нажмите на кнопку **Назад** в браузере.

## См. также:

Сценарий: Обнаружение устройств в сети ..... 1054

## Просмотр тегов, назначенных устройству

► *Чтобы просмотреть теги, назначенные устройству:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В появившемся окне свойств устройства откройте закладку **Теги**.

Отобразится список тегов, назначенных выбранному устройству.

Можно назначить другой тег (см. стр. 1162) устройству или удалить назначенный ранее тег (см. стр. 1162). Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

### См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Назначение тегов устройству вручную

► *Чтобы вручную назначить тег устройству:*

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег (см. стр. 1162).
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
   - Чтобы создать и добавить новый тег, выберите пункт **Создать тег** и укажите имя тега.
   - Чтобы выбрать существующий тег, выберите пункт **Назначить тег** и в раскрывающемся списке выберите нужный тег.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранный тег будет назначен устройству.

### См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Удаление назначенного тега с устройства

► *Чтобы снять назначенный тег с устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В появившемся окне свойств устройства откройте закладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.
5. В верхней части списка нажмите на кнопку **Отменить назначение тега**.
6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

> Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную (см. стр. 1161).
> Вы не можете вручную удалить теги, назначенные устройству программами или Агентом администрирования. Чтобы удалить эти теги, используйте утилиту klscflag (см. стр. 1167).

### См. также:

Сценарий: Обнаружение устройств в сети ..... 1054

## Просмотр правил автоматического назначения тегов устройствам

► *Чтобы просмотреть правила автоматического назначения тегов устройствам,*

Выполните одно из следующих действий:

- В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне программы перейдите в раздел **Устройства** → **Теги**, а затем перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству (см. стр. 1162), и нажмите на кнопку **Свойства**.

Отобразится список правил автоматического назначения тегов устройствам.

### См. также:

Сценарий: Обнаружение устройств в сети ..... 1054

## Изменение правил автоматического назначения тегов устройствам

► *Чтобы изменить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 1163).
2. Выберите правило, которое требуется изменить.

   Откроется окно с параметрами правила.
3. Измените основные параметры правила:
   a. В поле **Имя правила** измените название правила.

      Название не должно быть длиннее 256 символов.
   b. Выполните одно из следующих действий:
      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.
4. Выполните одно из следующих действий:

- Если вы хотите добавить новое условие, нажмите на кнопку **Добавить** и в открывшемся окне укажите параметры нового условия (см. стр. 1164).
- Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры (см. стр. 1164).
- Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.

5. В окне с параметрами правила нажмите на кнопку **OK**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

## См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Создание правил автоматического назначения тегов устройствам

► *Чтобы создать правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 1163).
2. Нажмите на кнопку **Добавить**.

   Откроется окно с параметрами нового правила.
3. Укажите основные параметры правила:
   a. В поле **Имя правила** введите название правила.

      Название не должно быть длиннее 256 символов.
   b. Выполните одно из следующих действий:
      - Включите правило, установив переключатель в положение **Правило включено**.
      - Выключите правило, установив переключатель в положение **Правило выключено**.
   c. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

      Название не должно быть длиннее 256 символов.
4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

   Откроется окно с параметрами нового условия.
5. Укажите название условия.

   Название не должно быть длиннее 256 символов. Название условия должно быть уникальным в рамках одного правила.
6. Настройте срабатывание правила по следующим условиям. Можно выбрать несколько условий.
   - **Сеть** – сетевые свойства устройства (например, имя устройства в сети Windows, принадлежность устройства к домену или к подсети IP-адресов).

Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Программы** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Active Directory** – нахождение устройства в подразделении Active Directory и членство устройства в группе Active Directory.
- **Реестр программ** – наличие на устройстве программ различных производителей.

7. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

   При необходимости можно задать несколько условий для одного правила. В этом случае тег будет назначен устройствам, если для них выполняется хотя бы одно из условий.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданное правило выполняется на устройствах, управляемых выбранным Сервером администрирования. Если параметры устройства соответствуют условиям правила, этому устройству назначается тег.

В дальнейшем правило применяется в следующих случаях:

- Автоматически, регулярно, в зависимости от загрузки сервера.
- После изменения правила (см. стр. 1163).
- После выполнения правила вручную (см. стр. 1165).
- После того как Сервер администрирования обнаружит изменения, которые соответствуют условиям правила, в параметрах устройства или в параметрах группы, которая содержит это устройство.

Вы можете создать несколько правил назначения тегов. Одному устройству может быть назначено несколько тегов, в случае если вы создали несколько правил назначения тегов и условия этих правил выполняются одновременно. Вы можете просмотреть список всех назначенных тегов (см. стр. 1162) в свойствах устройства.

## См. также:

Сценарий: Обнаружение устройств в сети.....1054

## Выполнение правил автоматического назначения тегов устройствам

Когда выполняется правило, тег, указанный в свойствах этого правила, назначается устройству, которое соответствует условиям, указанным в свойствах правила. Можно выполнять только активные правила.

► *Чтобы выполнить правила автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 1163).
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

## См. также:



## Удаление правил автоматического назначения тегов с устройств

► *Чтобы удалить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 1163).
2. Установите флажок напротив правила, которое требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Выбранное правило будет удалено. Тег, указанный в свойствах этого правила, будет снят со всех устройств, которым он был назначен.

> Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную (см. стр. 1161).

## См. также:



## Управление тегами устройств с помощью утилиты klscflag

В этом разделе содержится информация о том, как назначать или удалять теги устройств с помощью утилиты klscflag.

## В этом разделе



### *Назначение тега устройству*

Обратите внимание, что вам нужно запустить утилиту klscflag на клиентском устройстве, которому вы хотите назначить тег.

► *Чтобы назначить тег вашему устройству с помощью утилиты klscflag:*

1. Введите следующую команду, используя права администратора:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n
KLCONN_HOST_TAGS -sv "[\"TAG NAME\"]" -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

где `TAG NAME` – это имя тега, который вы хотите назначить устройству, например:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n
KLCONN_HOST_TAGS -sv "[\"ENTERPRISE\"]" -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

2. Перезапустите службу Агента администрирования.

Указанный тег будет назначен вашему устройству. Чтобы убедиться, что тег назначен успешно, просмотрите теги, назначенные устройству (см. стр. 1162).

Также можно назначать теги устройств вручную (см. стр. 1162).

### *Удаление тега устройства*

Если тег назначен устройству программой или Агентом администрирования, вы не сможете удалить этот тег вручную. В этом случае используйте утилиту klscflag для удаления назначенного тега с устройства.

Обратите внимание, что вам нужно запустить утилиту klscflag на клиентском устройстве, с которого вы хотите удалить тег.

► *Чтобы удалить тег с устройства с помощью утилиты klscflag:*

1. Введите следующую команду, используя права администратора:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n
KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

2. Перезапустите службу Агента администрирования.

Тег будет снят с устройства.

# Политики и профили политик

В Kaspersky Security Center 14.2 Web Console можно создавать политики для программ "Лаборатории Касперского" (см. стр. 69). В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

## См. также:



## В этом разделе



## О политиках и профилях политик

*Политика* – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 81) и ее подгруппам. Вы можете установить несколько программ "Лаборатории Касперского" (см. стр. 69) на устройства группы администрирования. Kaspersky Security Center предоставляет

по одной политике для каждой программы "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов (см. таблицу ниже):

*Таблица 89. Статус политики*

| Состояние | Описание |
|---|---|
| Активная | Это текущая политика, которая применяется к устройству. Для программы "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики программы "Лаборатории Касперского" применяются к устройству. |
| Неактивная | Политика, которая в настоящее время не применяется к устройству. |
| Для автономных пользователей | Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации. |

Политики действуют по следующим правилам:

- Для одной программы можно настроить несколько политик с различными значениями.
- Для одной программы может быть активна только одна политика.
- Вы можете активировать неактивную политику при возникновении определенного события. Например, в период вирусных атак можно включить параметры для усиленной антивирусной защиты.
- Политика может иметь дочерние политики.

Вы можете использовать политики для подготовки к экстренным ситуациям, например, к вирусной атаке. Например, если происходит атака через флеш-накопители USB, можно активировать политику, блокирующую доступ к флеш-накопителям. В этом случае текущая активная политика автоматически становится неактивной.

Чтобы не поддерживать большое число политик, например, когда в разных случаях предполагается изменение только нескольких параметров, вы можете использовать профили политик.

*Профиль политики* – это именованное подмножество параметров политики, которые заменяют значения параметров политики. Профиль политики влияет на формирование эффективных параметров управляемого устройства. *Эффективные параметры* – это набор параметров политики, параметров профиля политики и параметров локальной программы, которые в настоящее время применяются к устройству.

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.
- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

### См. также:

Наследование политик и профилей политик .....1170

## Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (). В таблице ниже показаны состояния значка замка:

Таблица 90. Статусы значка замка

| Состояние | Описание |
|---|---|
|  | Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемой программы. Такие параметры называются *разблокированными*. |
|  | Если рядом с параметром отображается закрытый значок замка и переключатель включен, параметр применяется к устройствам, на которых применяется политика. Пользователь не может изменять значения этих параметров в интерфейсе управляемой программы. Такие параметры называются *заблокированными*. |

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами программы "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

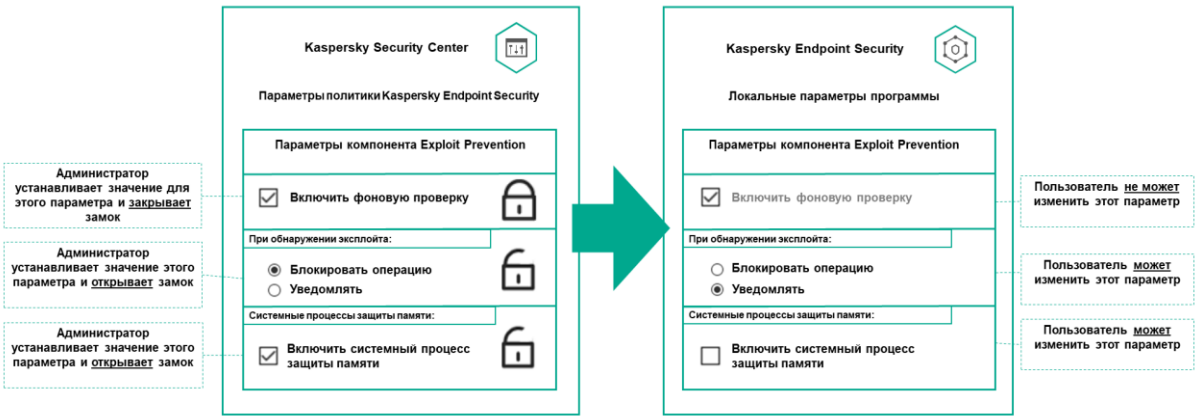
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров программы "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров программы "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемая программа "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры программы "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже).



kaspersky

## См. также:



## Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

## В этом разделе



## Иерархия политик

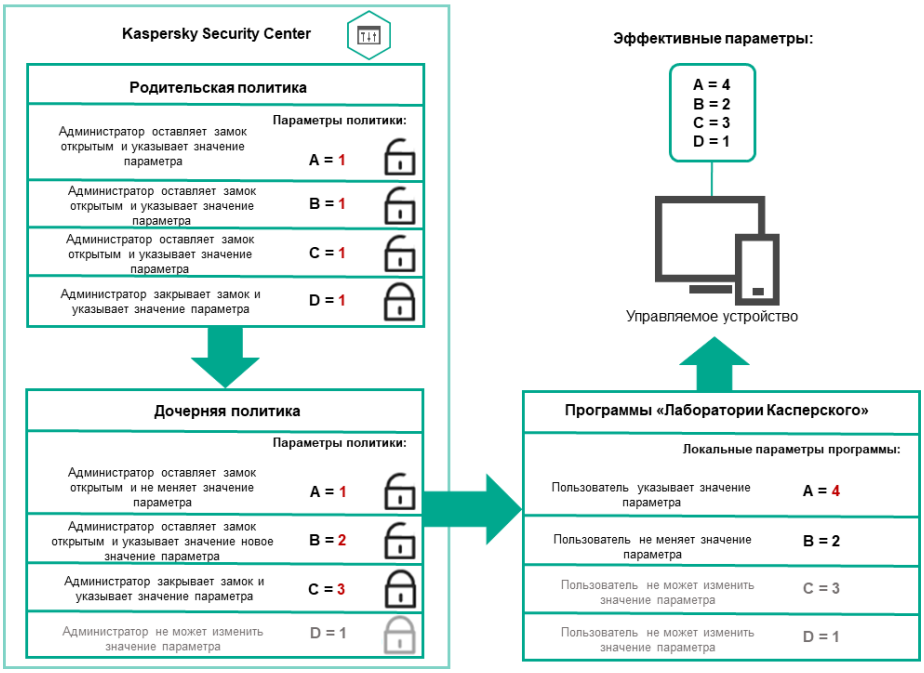
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования (см. стр. 81). Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

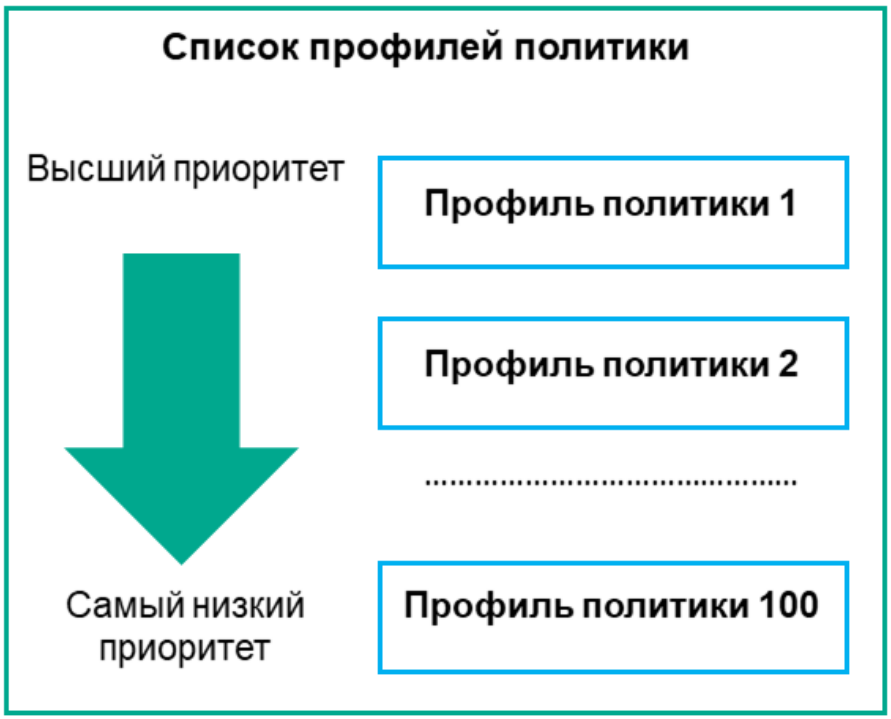
Политики одной и той же программы действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).



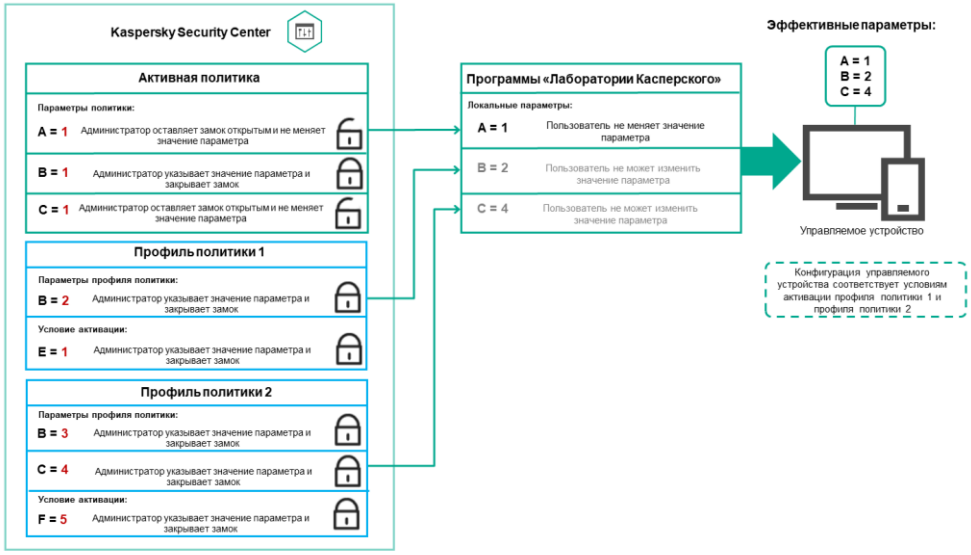

## Профили политик в иерархии политик

Профили политики имеют следующие условия назначения приоритета:

- Положение профиля в списке профилей политики обозначает его приоритет. Вы можете изменить приоритет профиля политики. Самая высокая позиция в списке обозначает самый высокий приоритет (см. рисунок ниже).



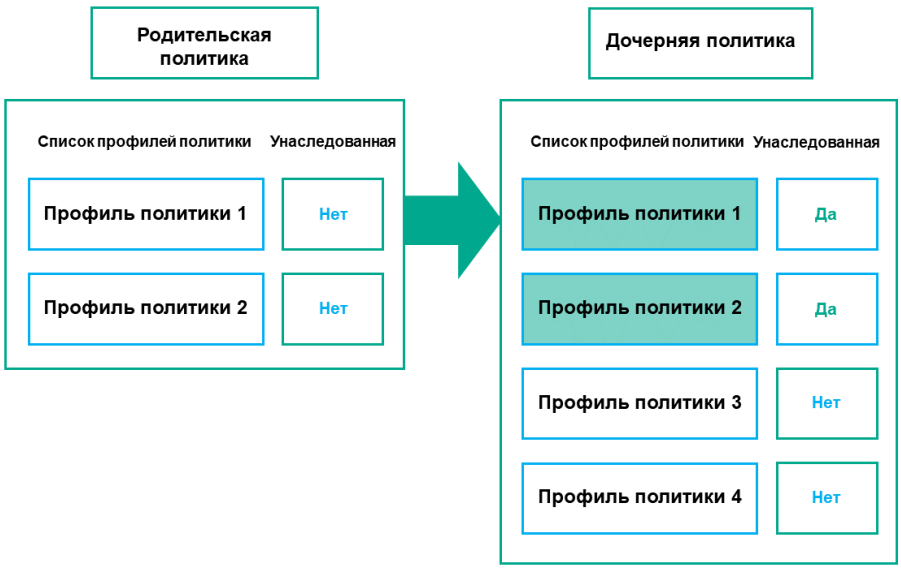
- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).




### Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

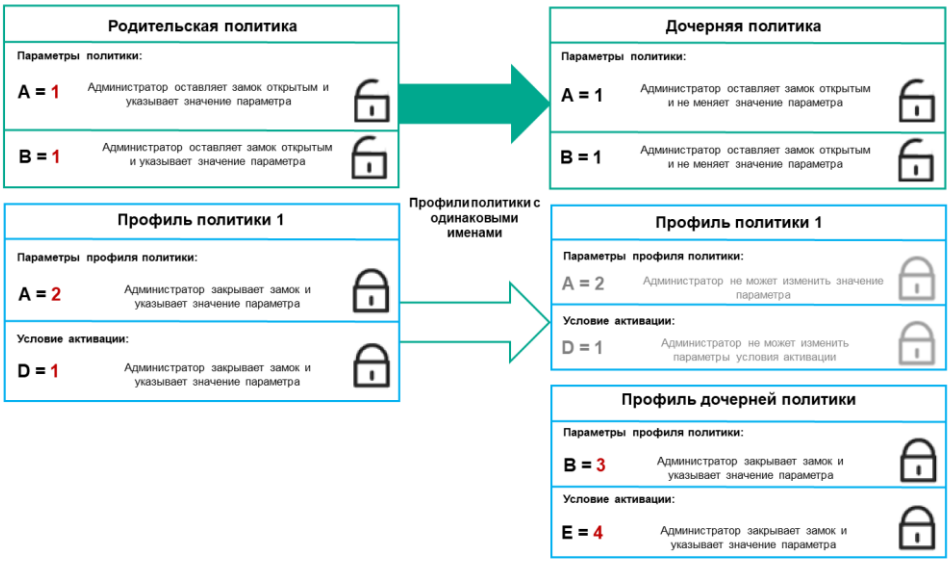
- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.
- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).




### Профили политики с одинаковыми именами

Если на разных уровнях иерархии есть две политики с одинаковыми именами, эти политики работают в соответствии со следующими правилами:

- Заблокированные параметры и условие активации профиля для профиля политики более высокого уровня изменяют параметры и условие активации профиля для профиля политики более низкого уровня (см. рисунок ниже).




- Разблокированные параметры и условие активации профиля для профиля политики более высокого уровня не изменяют параметры и условие активации профиля для профиля политики более низкого уровня.

## См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

## Как реализуются параметры управляемого устройства

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемой программы.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

## См. также:

О политиках и профилях политик.....1167

Блокировка (замок) и заблокированные параметры .....1168

Иерархия политик .....1170

Профили политик в иерархии политик.....1171

kaspersky

## Управление политиками

В этом разделе описывается управление политиками и дается информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

### В этом разделе



### Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

► *Чтобы просмотреть список политик:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

### См. также:


Сценарий: Настройка защиты сети ..... 400


### Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

► *Чтобы создать политику:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.

2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбор программы**.

3. Выберите программу, для которой требуется создать политику.
4. Нажмите на кнопку **Далее**.

   Откроется окно параметров новой политики на закладке **Общие**.

5. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.
6. Перейдите на закладку **Свойства программы**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.

7. В левой области закладки **Свойства программы** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от программы, для которой вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования (см. стр. 980)
   - Параметры политики Агента администрирования (см. стр. 750)
   - Документация Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.5.0/ru-RU/

   Подробнее о параметрах других программ безопасности см. в документации к соответствующей программе.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

В результате добавленная политика отображается в списке политик.

## См. также:

Сценарий: Развертывание программ "Лаборатории Касперского" .....1035

Настройка и распространение политик: подход, ориентированный на устройства .....402

Сценарий: Настройка защиты сети .....400

## Изменение политики

► *Чтобы изменить политику:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.

3. Укажите общие параметры (см. стр. 1176) и параметры программы, для которой вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования (см. стр. 980)
   - Параметры политики Агента администрирования (см. стр. 750)

- Документация Kaspersky Endpoint Security для Windows
  https://help.kaspersky.com/KESWin/11.5.0/ru-RU/

Подробнее о параметрах других программ безопасности см. в документации к этим программам.

4. Нажмите на кнопку **Сохранить**.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Общие параметры политик

**Общие**

На закладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная**

    Если выбран этот вариант, политика становится активной.

    По умолчанию выбран этот вариант.
  - **Для автономных пользователей**

    Если выбран этот вариант, политика начинает действовать при выходе устройства из сети организации.
  - **Неактивная**

    Если выбран этот вариант, политика становится неактивной, но сохраняется в папке **Политики**. При необходимости ее можно сделать активной.
- В блоке **Наследование параметров** можно настроить параметры наследования политики:
  - **Наследовать параметры из политики верхнего уровня**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:

    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

**Настройка событий**

В разделе **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое событие**

  Раздел **Критическое событие** не отображается в свойствах политики Агента администрирования.

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке событий отображаются названия событий и время хранения событий на Сервере администрирования по умолчанию (в днях). Нажав на тип события, вы можете указать следующие параметры:

- **Регистрация событий**

  Вы можете указать количество дней хранения событий и выбрать, где хранить события:

  - **Экспортировать в SIEM-систему по протоколу Syslog**
  - **В журнале событий ОС на устройстве**
  - **В журнале событий ОС на Сервере администрирования**

- **Уведомления о событиях**

  Вы можете выбрать способ уведомления о событии:

  - **Уведомлять по электронной почте**
  - **Уведомлять по SMS**
  - **уведомлять запуском исполняемого файла или скрипта**
  - **Уведомлять по SNMP**

  По умолчанию используются параметры уведомлений, указанные на закладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на закладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

**История ревизий**

На закладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат (см. стр. 1108).

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Включение и выключение параметра наследования политики

► *Чтобы включить или выключить параметр наследования в политике:*

1. Откройте требуемую политику.
2. Откройте закладку **Общие**.
3. Включите или выключите наследования политики:

- Если вы включили **Наследовать параметры родительской политики** для дочерней политики и заблокировали некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры для дочерней группы.
- Если вы выключили **Наследовать параметры родительской политики** для дочерней политики, тогда вы можете изменить все параметры в дочерней группе, даже если некоторые параметры заблокированы в родительской политике.
- Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, это включит параметр **Наследовать параметры родительской политики** для каждой дочерней политики. В этом случае вы не можете выключить этот параметр для дочерних политик. Все параметры, которые заблокированы в родительской политике, принудительно наследуются в дочерних группах, и вы не можете изменить эти параметры в дочерних группах.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, или нажмите на кнопку **Отмена**, чтобы отменить изменения.

По умолчанию параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

### См. также:

Иерархия политик ..... 1170
Общие параметры политик ..... 748
Сценарий: Настройка защиты сети ..... 400

## Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

► *Чтобы скопировать политику в другую группу администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется скопировать.
3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).
5. Нажмите на кнопку **Копировать** внизу экрана.
6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, то к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

kaspersky

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

► *Чтобы переместить политику в другую группу администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется переместить.
3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).
5. Нажмите на кнопку **Переместить** в верху экрана.
6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Если политика не унаследована из группы источника, она будет перемещена в целевую группу со всем профилями политики. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активная** в любое время.

Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, то к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Экспорт политики

Kaspersky Security Center позволяет сохранить политику, ее параметры и профили политики в файл KLP. Вы можете использовать файл KLP для импорта сохраненной политики (см. стр. 1180) как в Kaspersky Security Center Windows, так и в Kaspersky Security Center Linux.

► *Чтобы экспортировать политику:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок рядом с политикой, которую вы хотите экспортировать.

   Невозможно экспортировать несколько политик одновременно. Если вы выберете более одной политики, кнопка **Экспортировать** будет неактивна.

3. Нажмите на кнопку **Экспортировать**.
4. В открывшемся окне **Сохранить как** укажите имя файла политики и путь. Нажмите на кнопку **Сохранить**.

   Окно **Сохранить как** отображается только в том случае, если вы используете Google Chrome, Microsoft Edge или Opera. Если вы используете другой браузер, файл политики автоматически сохраняется в папку **Загрузки**.

## Импорт политики

Kaspersky Security Center позволяет импортировать политику из файла KLP. Файл KLP содержит экспортированную политику (см. стр. 1179), ее параметры и профили политики.

► *Чтобы импортировать политику:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Импортировать**.
3. Нажмите на кнопку **Обзор**, чтобы выбрать файл политики, который вы хотите импортировать.
4. В открывшемся окне укажите путь к файлу политики KLP и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл политики.

   Начнется обработка политики.
5. После успешной обработки политики выберите группу администрирования, к которой вы хотите применить политику.
6. Нажмите на кнопку **Завершить**, чтобы завершить импорт политики.

Появится уведомление с результатами импорта. Если политика успешно импортирована, вы можете перейти по ссылке **Подробнее** для просмотра свойств политики.

После успешного импорта политика отображается в списке политик. Также импортируются параметры и профили политики. Независимо от статуса политики, выбранной при экспорте, импортируемая политика неактивна. Вы можете изменить статус политики в свойствах политики.

Если имя новой импортированной политики идентично имени существующей политики, имя импортированной политики расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

## Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

► *Чтобы просмотреть статус применения политики на каждом устройстве:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.
3. В появившемся меню выберите ссылку **Результаты применения**.

Откроется окно **Результат распространения <название политики>**.

4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100 000.

► *Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.
3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на закладке **Общие**.
2. Выберите раздел **Вирусная атака**.
3. В правой панели нажмите на ссылку **Настроить активацию политик по возникновению события "Вирусная атака"**.

   Откроется окно **Активации политик**.
4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам записью и затем нажмите на кнопку **Добавить**.

   Откроется окно с группой администрирования **Управляемые устройства**.
5. Нажмите на значок шеврона ( ) рядом с **Управляемые устройства**.

   Отобразится иерархия групп администрирования и их политик.
6. В иерархии групп администрирования и их политик нажмите на имя политики (или политик), которая активируется при возникновении вирусной атаки.

   Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.
7. Нажмите на кнопку **Сохранить**.

   Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

Сценарий: Настройка защиты сети .....400

## Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

► *Чтобы удалить политику:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок рядом с политикой, которую вы хотите удалить, и нажмите на кнопку **Удалить**.

   Кнопка **Удалить** становится неактивной (серой), если вы выбрали унаследованную политику.
3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика и все ее профили политики удалены.

### См. также:

Сценарий: Настройка защиты сети .....400

# Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, изменении профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

kaspersky

## В этом разделе



## Просмотр профилей политики

► *Чтобы просмотреть профили политики:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на закладке **Общие**.
3. Откройте закладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

## См. также:


Сценарий: Настройка защиты сети ..... 400


## Изменение приоритета профиля политики

► *Чтобы изменить приоритет профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики.
2. На закладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.
3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

   Чем выше расположен профиль политики в списке, тем выше его приоритет.
4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

## См. также:

Профили политик в иерархии политик....1171
Наследование политик и профилей политик....1170
Сценарий: Настройка защиты сети....400

## Создание профиля политики

► *Чтобы создать профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. Нажмите на кнопку **Добавить**.
3. Если необходимо, измените заданные по умолчанию имя и параметры наследования профиля политики.
4. Перейдите на закладку **Свойства программы**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.

5. В левой области закладки **Свойства программы** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля политики.

Профиль политики отобразится в списке профилей политики.

## См. также:

Настройка и распространение политик: подход, ориентированный на устройства....402
Сценарий: Настройка защиты сети....400

## Изменение профиля политики

Изменение профиля доступно только для политик Kaspersky Endpoint Security для Windows.

► *Чтобы изменить профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики.

2. На закладке **Профили политики** нажмите на профиль политики, который вы хотите изменить.

   В результате откроется окно свойств профиля политики.

3. В окне свойств настройте параметры профиля:
   - Если необходимо, на закладке **Общие** измените имя профиля политики и включите или выключите профиль.
   - Измените правила активации профиля политики (см. стр. 1186).
   - Измените остальные параметры.

   Подробнее о параметрах программ безопасности см. в документации к соответствующей программе.
4. Нажмите на кнопку **Сохранить**.

Измененные параметры начнут действовать после синхронизации устройства с Сервером администрирования (если профиль политики активен) либо после выполнения правила активации (если профиль политики неактивен).

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Копирование профиля политики

Вы можете скопировать профиль политики в текущую политику или в другую политику, например, если вы хотите иметь идентичные профили политик для разных политик. Вы также можете использовать копирование, если хотите иметь два или более профилей политики, которые отличаются небольшим количеством параметров.

► *Чтобы скопировать профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.
2. На закладке **Профили политик** выберите профиль, который требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне выберите политику, в которую требуется скопировать профиль политики.

   Вы можете скопировать профиль политики в эту же политику или в политику, которую вы выбрали.
5. Нажмите на кнопку **Копировать**.

Профиль политики скопирован в политику, которую вы выбрали. Новый скопированный профиль политики имеет самый низкий приоритет. Если вы скопировали профиль политики в эту же политику, к имени такого профиля добавляется окончание вида (<порядковый номер>), например: (1), (2).

Позже вы можете изменить параметры профиля политики, включая его имя и приоритет. В этом случае исходный профиль политики не будет изменен.

## См. также:

Сценарий: Настройка защиты сети ..... 400

## Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики.

2. На закладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики (см. стр. 1184).

3. На закладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   - **Общие правила активации профиля политики**

     Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

     Для этого параметра на следующем шаге укажите:

     - **Статус устройства**

       Определяет условие присутствия устройства в сети:

       - **В сети** – устройство находится в сети, Сервер администрирования доступен.
       - **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
       - **N/A** – критерий не применяется.

     - **Правило подключения к Серверу администрирования активно на этом устройстве**

       Выберите условие для активации профиля политики (независимо от того, выполняется ли это правило или нет) и выберите имя правила.

       Правило определяется сетевым местоположением устройства для подключения к Серверу администрирования, при выполнении или невыполнении условий которого профиль политики будет активирован.

       Описание сетевого местоположения устройств для подключения к Серверу администрирования можно создать или настроить в правиле переключения Агента администрирования.

   - **Правила для определенного владельца устройства**

     Для этого параметра на следующем шаге укажите:

     - **Владелец устройства**

       Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- устройство принадлежит указанному владельцу (знак "=");

- устройство не принадлежит указанному владельцу (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  - **Владелец устройства включен во внутреннюю группу безопасности**

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

- владелец устройства является членом указанной группы безопасности (знак "=");
- владелец устройства не является членом указанной группы безопасности (знак "#").

  Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать группу безопасности Kaspersky Security Center. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для характеристик оборудования**

  Установите флажок, чтобы настроить условие активации на устройстве в зависимости от объема памяти и количества логических процессоров устройства.

  Для этого параметра на следующем шаге укажите:

  - **Объем оперативной памяти (МБ)**

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по объему оперативной памяти устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - объем оперативной памяти устройства меньше указанного значения (знак "<");
    - объем оперативной памяти устройства больше указанного значения (знак ">").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать объем оперативной памяти устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  - **Количество логических процессоров**

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по количеству логических процессоров устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:

    - количество логических процессоров устройства меньше или равно указанному значению (знак "<");
    - количество логических процессоров устройства больше или равно указанному значению (знак ">").

    Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать количество логических процессоров устройства. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Правила для назначения роли**

  Для этого параметра на следующем шаге укажите:

**Активировать профиль политики по наличию роли у владельца устройства**

Включите этот параметр, чтобы настроить и включить правило активации профиля политики на устройстве в зависимости от наличия определенной роли (см. стр. 771) у его владельца. Добавить роль вручную из списка существующих ролей.

Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием.

- **Правила для использования тега**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от тегов, назначенных устройству. Вы можете активировать профиль политики либо на устройствах, которые имеют выбранные теги, либо не имеют их.

Для этого параметра на следующем шаге укажите:

- **Тег**

  В списке тегов задайте правило включения устройств в профиль политики, установив флажки нужным тегам.

  Вы можете добавить в список новые теги, введя их в поле над списком и нажав на кнопку **Добавить**.

  В профиль политики будут включены устройства, в описании которых есть все выбранные теги. Если флажки сняты, критерий не применяется. По умолчанию флажки сняты.

- **Применять к устройствам без выбранных тегов**

  Включите параметр, если необходимо инвертировать выбор тегов.

  Если параметр включен, в профиль политики будут включены устройства, в описании которых нет выбранных тегов. Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

- **Правила использования Active Directory**

  Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от размещения устройства в подразделении Active Directory или же от членства устройства или его владельца в группе безопасности Active Directory.

Для этого параметра на следующем шаге укажите:

- **Членство владельца устройства в группе безопасности Active Directory**

  Если параметр включен, профиль политики активируется на устройстве, владелец которого является членом указанной группы безопасности. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Членство устройства в группе безопасности Active Directory**

Если параметр включен, профиль политики активируется на устройстве. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- **Размещение устройства в подразделении Active Directory**

  Если параметр включен, профиль политики активируется на устройстве входит в указанное подразделение Active Directory. Если параметр выключен, критерий активации профиля не применяется.

  По умолчанию параметр выключен.

От выбора параметров на этом шаге зависит дальнейшее количество окон мастера. Вы можете изменить правила активации профиля политики позже.

1. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики в разделе **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

### См. также:

Настройка и распространение политик: подход, ориентированный на устройства .....402

Сценарий: Настройка защиты сети .....400

## Удаление профиля политики

► *Чтобы удалить профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 1183).

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.
3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых программ, установленных на устройствах групп нижнего уровня.

### См. также:

Сценарий: Настройка защиты сети .....400

kaspersky

# Пользователи и роли пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

## В этом разделе



## См. также:



## О ролях пользователей

*Роль пользователя* (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами программ "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп безопасности на любом уровне иерархии групп администрирования, Серверов администрирования либо на уровне конкретных объектов (см. стр. 1216).

Если вы управляете устройствами через иерархию Серверов администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только с главного Сервера администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы (см. стр. 799).

Вы можете связывать роли с профилями политик. Если пользователю назначена роль, этот пользователь получает параметры безопасности, требуемые для выполнения служебных обязанностей.

Роль пользователя может быть связана с устройствами пользователей заданной группы администрирования.

kaspersky

**Область роли пользователя**

*Область роли пользователя* – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

**Преимущество использования ролей**

Преимущество использования ролей заключается в том, что вам не нужно указывать параметры безопасности для каждого управляемого устройства или для каждого из пользователей отдельно. Количество пользователей и устройств в компании может быть большим, но количество различных функций работы, требующих разных настроек безопасности, значительно меньше.

**Отличия от использования профилей политики**

Профили политики – это свойства политики, созданной для каждой программы "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных программ. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

## См. также:

Сценарий: Настройка защиты сети ..... 400

# Настройка прав доступа к функциям программы. Управление доступом на основе ролей

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых программ "Лаборатории Касперского".

Вы можете настроить права доступа к функциям программы (см. стр. 1192) для пользователей Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей (см. стр. 1190) с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к программе. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В программе можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли (см. стр. 1212) пользователей с уже настроенным набором прав или создавать роли (см. стр. 1222) и самостоятельно настраивать необходимые права.

## В этом разделе



## См. также:

Сценарий: Настройка защиты сети ..... 400

kaspersky

## Права доступа к функциям программы

В таблице ниже приведены функции Kaspersky Security Center с правами доступа для управления задачами, отчетами, параметрами и для выполнения действий пользователя.

Для выполнения действий пользователя, перечисленных в таблице, у пользователя должно быть право, указанное рядом с действием.

Права на **Чтение**, **Запись** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общий функционал**: функциональная область **Базовая функциональность**.

*Таблица 91. Права доступа к функциям программы*

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **Общие функции**: **Управление группами администрирования.** | **Запись.** | • Добавление устройства в группу администрирования: **Запись.**<br>• Удаление устройства из состава группы администрирования: **Запись.**<br>• Добавление группы администрирования в другую группу администрирования: **Запись.**<br>• Удаление группы администр | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | ирования из другой группы администрирования: **Запись.** | | | |
| **Общие функции**: **Доступ к объектам независимо от их списков ACL.** | **Чтение.** | Получение доступа на чтение ко всем объектам: **Чтение.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Базовая функциональность.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**.<br>• Получение мобильного протокола пользовательского сертифика | • Загрузка обновлений в хранилище Сервера администрирования.<br>• Рассылка отчетов.<br>• Распространение инсталляционных пакетов.<br>• Установка программ на подчиненные Серверы администрирования. | • Отчет о состоянии защиты.<br>• Отчет об угрозах.<br>• Отчет о наиболее заражаемых устройствах.<br>• Отчет о статусе антивирусных баз.<br>• Отчет об ошибках.<br>• Отчет о сетевых атаках.<br>• Сводный отчет о программах для защиты почтовых систем.<br>• Сводный отчет о | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | та (LWNGT): **Чтение.**<br>• Установка мобильного протокола пользовательского сертификата (LWNGT): **Запись.**<br>• Получить список сетей, определенных NLA: **Чтение.**<br>• Добавить, изменить или удалить список сетей, определенных NLA: **Запись.**<br>• Просмотр списка контроля доступа групп: **Чтение.**<br>• Просмотрите журнал событий Kaspersky Event Log: **Чтение.** | | программах для защиты периметра.<br>• Сводный отчет о типах программ.<br>• Отчет о пользователях зараженных устройств.<br>• Отчет об инцидентах.<br>• Отчет о событиях.<br>• Отчет о работе точек распространения.<br>• Отчет о подчиненных Серверах администрирования.<br>• Отчет о событиях Контроля устройств.<br>• Отчет об уязвимостях.<br>• Отчет о запреще | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | | | нных программах.<br>• Отчет о работе Веб-Контроля.<br>• Отчет о статусе шифрования управляемых устройств.<br>• Отчет о статусе шифрования запоминающих устройств.<br>• Отчет об ошибках шифрования.<br>• Отчет о блокировании доступа к зашифрованным файлам.<br>• Отчет о правах доступа к зашифрованным устройствам.<br>• Отчет об эффективных | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | | | правах пользователя.<br>• Отчет о правах. | |
| **Общие функции**: **Удаленные объекты.** | • **Чтение.**<br>• **Запись.** | • Просмотр удаленных объектов в корзине: **Чтение.**<br>• Удаление объектов из корзины: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Обработка событий.** | • **Удаление событий.**<br>• **Изменение параметров уведомления о событиях.**<br>• **Изменение параметров записи событий в журнал событий.**<br>• **Запись.** | • Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий.**<br>• Изменение параметров уведомления о событиях: **Изменение параметров уведомления о** | Отсутствует. | Отсутствует. | Параметры:<br>• Параметры вирусной атаки: количество обнаружений вирусов, необходимое для создания события вирусной атаки.<br>• Параметры вирусной атаки: период для оценки обнаружения вирусов.<br>• Максимальное количество событий, хранящихся в базе данных. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **событиях**.<br>• Удаление событий: **Удаление событий.** | | | • Период хранения событий удаленных устройств. |
| **Общие функции**: **Операции с Сервером администрирования.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Изменение списков ACL объекта.**<br>• **Выполнение действий над выборками устройств.** | • Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись.**<br>• Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись.**<br>• Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись.** | • Резервное копирование данных Сервера администрирования.<br>• Обслуживание базы данных. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись.**<br>• Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись.**<br>• Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись.**<br>• Изменение портов Сервера администрирования для подключения | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | мобильных устройств: **Запись.**<br>• Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. **Запись.**<br>• Укажите максимальное количество событий, которое может отправлять Сервер администрирования. **Запись.**<br>• Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись.** | | | |
| **Общие функции**: **Развертывание программ "Лаборатор** | • **Управление патчами "Лаборатории** | Одобрить или отклонить установку патча: **Управление патчами** | Отсутствует. | • Отчет об использовании лицензионных ключей | Инсталляционный пакет: "Лаборатория Касперского". |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| **ии Касперского".** | **Касперского".**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | **"Лаборатории Касперского".** | | виртуальным Сервером администрирования.<br>• Отчет о версиях программ "Лаборатории Касперского".<br>• Отчет о несовместимых программах.<br>• Отчет о версиях обновлений модулей программ "Лаборатории Касперского".<br>• Отчет о развертывании защиты. | |
| **Общие функции**: **Управление лицензионными ключами.** | • **Экспорт файл ключа.**<br>• **Запись.** | • Экспорт файл ключа: **Экспорт файл ключа.**<br>• Изменение параметров лицензионного | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | ключа Сервера администрирования: **Запись.** | | | |
| **Общие функции**: **Управление отчетами.** | • **Чтение.**<br>• **Запись.** | • Создание отчетов для объектов независимо от их списков ACL: **Запись.**<br>• Выполнять отчеты независимо от их списков ACLs: **Чтение.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Иерархия Серверов администрирования** | **Настройка иерархии Серверов администрирования** | Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Общие функции**: **Права пользователя.** | **Изменение списков ACL объекта.** | • Изменение свойств Безопасности любого объекта: **Изменение списков ACL объекта.** | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | • Управление ролями пользователей: **Изменение списков ACL объекта.**<br>• Управление внутренними пользователями: **Изменение списков ACL объекта.**<br>• Управление группами безопасности: **Изменение списков ACL объекта.**<br>• Управление псевдонимами: **Изменение списков ACL объекта.** | | | |
| **Общие функции**: **виртуальные Серверы администрирования;** | • **Управление виртуальными Серверами администрирования.** | • Получение списка виртуальных Серверов администрирования: **Чтение.**<br>• Получение | Отсутствует. | Отчет о результатах установки обновлений стороннего ПО. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | информации о виртуальном Сервере администрирования: **Чтение.**<br>• Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования.**<br>• Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами администрирования.** | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования.** | | | |
| **Общие функции**: **Управление ключами шифрования** | **Запись.** | Импорт ключей шифрования: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Управление мобильными устройствами**: **Общие** | • **Подключение новых устройств.**<br>• **Отправка только информационных команд на мобильные устройства.**<br>• **Отправка команд на мобильные устройства.**<br>• **Управление** | • Получение восстановленных данных службы управления ключами: **Чтение.**<br>• Удаление сертификатов пользователей: **Управление сертификатами.**<br>• Получение | Отсутствует. | Отсутствует. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | **сертификатами.**<br>• **Чтение.**<br>• **Запись.** | публичной части сертификата пользователя: **Чтение.**<br>• Проверка, включена ли инфраструктура открытых ключей: **Чтение.**<br>• Проверка учетной записи инфраструктуры открытых ключей: **Чтение.**<br>• Получение шаблонов инфраструктуры открытых ключей: **Чтение.**<br>• Получение шаблонов инфраструктуры открытых ключей с помощью расширенного использования ключа (EKU) | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | сертификата: **Чтение.**<br>• Проверка, не отозвали сертификат инфраструктуры открытых ключей: **Чтение.**<br>• Обновление параметров выпуска сертификатов пользователя: **Управление сертификатами.**<br>• Получение параметров выпуска сертификатов пользователя: **Чтение.**<br>• Получение пакетов по названию и версиям программ: **Чтение.**<br>• Установка или отмена сертифика | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | тов пользователя: **Управление сертификатами.**<br>• Обновление сертификата пользователя: **Управление сертификатами.**<br>• Установка тега для сертификата пользователя: **Управление сертификатами.**<br>• Запуск генерации инсталляционного пакета, содержащего iOS MDM-профиль; отмена генерации инсталляционного пакета, содержащего iOS MDM-профиль: | | | |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **Подключение новых устройств.** | | | |
| **Управление системой**: **Подключения.** | • **Запуск RDP-сессий.**<br>• **Подключение к существующим RDP-сессиям.**<br>• **Туннелирование.**<br>• **Сохранение файлов с устройства на рабочем месте администратора.**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Создание сеанса совместного доступа к рабочему столу: **Право на создание сеанса совместного доступа к рабочему столу.**<br>• Создание RDP-сессии: **Подключение к существующим RDP-сессиям.**<br>• Создание туннеля: **Туннелирование.**<br>• Сохранение списка сетей: **Сохранение файлов с устройств на рабочем месте** | Отсутствует. | Отчет о пользователях устройства. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | **администратора.** | | | |
| **Управление системой**: **Инвентаризация оборудования** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Получение или экспорт объектов инвентаризации оборудования: **Чтение.**<br>• Добавление, установка или удаление объектов инвентаризации оборудования: **Запись.** | Отсутствует. | • Отчет о реестре оборудования.<br>• Отчет об изменении конфигурации.<br>• Отчет об оборудовании. | Отсутствует. |
| **Управление системой**: **Управление доступом в сеть.** | • **Чтение.**<br>• **Запись.** | • Просмотр параметров Cisco: **Чтение.**<br>• Изменение параметров Cisco: **Запись.** | Отсутствует. | Отсутствует. | Отсутствует. |
| **Управление системой**: **Развертывание операционной системы.** | • **Развертывание PXE-серверов.**<br>• **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборкам** | • Развертывание PXE-серверов: **Развертывание PXE-серверов.**<br>• Просмотр списка PXE-серверов: **Чтение.** | Создание инсталляционного пакета на основе образа ОС эталонного устройства. | Отсутствует. | Инсталляционный пакет: Образ операционной системы. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | **и устройств.** | • Запуск или остановка процесс установки на PXE-клиентах: **Выполнение.**<br>• Управление драйверами для среды WinPE и образов операционной системы: **Запись.** | | | |
| **Управление системой**: **Системное администрирование.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Просмотр свойства патчей сторонних производителей: **Чтение.**<br>• Изменение свойства патчей сторонних производителей: **Запись.** | • Выполнение синхронизации обновлений Центра обновления Windows.<br>• Установка обновлений Центра обновления Windows.<br>• Закрытие уязвимостей.<br>• Установка требуемых обновлений и закрытия | Отчет об обновлениях ПО. | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | | уязвимостей. | | |
| **Управление системой**: **Удаленная установка** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | • Просмотр Системного администрирования стороннего производителя на основе свойств инсталляционного пакета: **Чтение.**<br>• Изменение Системного администрирования на основе свойств инсталляционного пакета: **Запись.** | Отсутствует. | Отсутствует. | Инсталляционные пакеты:<br>• "Пользовательская программа".<br>• Инсталляционный пакет. |
| **Управление системой**: **Инвентаризация программ.** | • **Чтение.**<br>• **Запись.**<br>• **Выполнение.**<br>• **Выполнение действий над выборками устройств.** | Отсутствует. | Отсутствует. | • Отчет об установленных программах.<br>• Отчет об истории реестра программ.<br>• Отчет о состоянии групп лицензионных | Отсутствует. |

| Функциональная область | Право | Действие пользователя: право, необходимое для выполнения действия | Задача | Отчет | Другое |
|---|---|---|---|---|---|
| | | | | программ.<br>• Отчет о лицензионных ключах сторонних программ. | |

## См. также:

Сценарий: Настройка защиты сети .....400

## Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям программы (см. стр. 771).

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных ролей пользователей, доступных в Kaspersky Security Center, могут быть связаны с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер** (эти роли присутствуют в Kaspersky Security Center начиная с версии 11). Права доступа этих ролей предварительно настраиваются в соответствии со стандартными задачами и обязанностями соответствующих должностей. В таблице ниже показано как роли могут быть связаны с определенными должностями.

*Таблица 92. Примеры ролей для определенных должностей*

| Роль | Комментарий |
|---|---|
| Аудитор | Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права **Чтение** и **Запись** для области **Удаленные объекты**). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации. |
| Контролер | Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации. |

| Роль | Комментарий |
|---|---|
| Специалист по безопасности | Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации. |

В таблице ниже приведены права для каждой предопределенной роли пользователя.

*Таблица 93. Права предопределенных ролей пользователей*

| Роль | Описание |
|---|---|
| Администратор Сервера администрирования | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Обработка событий.**<br>  • **Иерархия Серверов администрирования.**<br>  • **Виртуальные Серверы администрирования.**<br>• **Управление системой**:<br>  • **Подключения.**<br>  • **Инвентаризация оборудования.**<br>  • **Инвентаризация программ.**<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Оператор Сервера администрирования | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Виртуальные Серверы администрирования.**<br>• **Управление системой**:<br>  • **Подключения.**<br>  • **Инвентаризация оборудования.**<br>  • **Инвентаризация программ.** |
| Аудитор | Разрешает все операции в функциональной области **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Удаленные объекты.**<br>• **Управление отчетами.**<br>Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации. |

| Роль | Описание |
| --- | --- |
| Администратор установки программ | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Развертывание программ "Лаборатории Касперского".**<br>  • **Управление лицензионными ключами.**<br>• **Управление системой**:<br>  • **Развертывание операционной системы.**<br>  • **Системное администрирование.**<br>  • **Удаленная установка**<br>  • **Инвентаризация программ.**<br>Предоставляет права на **Чтение** и **Выполнение** в области **Общий функционал**: функциональная область **Виртуальные Серверы администрирования**. |
| Оператор установки программ | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Развертывание программ "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области).<br>  • **Виртуальные Серверы администрирования.**<br>• **Управление системой**:<br>  • **Развертывание операционной системы.**<br>  • **Системное администрирование.**<br>  • **Удаленная установка.**<br>  • **Инвентаризация программ.** |
| Администратор Kaspersky Endpoint Security | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• Область Kaspersky Endpoint Security, включая все функции.<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Оператор Kaspersky Endpoint Security | Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• Область Kaspersky Endpoint Security, включая все функции. |

| Роль | Описание |
|---|---|
| Главный администратор | Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Управление отчетами.**<br>Предоставляет права на **Чтение** и **Запись** в области **Общий функционал**: **Управление ключами шифрования**. |
| Главный оператор | Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях:<br>• **Общие функции**:<br>  • **Базовая функциональность.**<br>  • **Удаленные объекты.**<br>  • **Операции с Сервером администрирования.**<br>  • **Развертывание программ "Лаборатории Касперского"**<br>  • **Виртуальные Серверы администрирования.**<br>• **Управление мобильными устройствами: Общие**<br>• **Управление системой**, включая все функции.<br>• Область Kaspersky Endpoint Security, включая все функции. |
| Администратор управления мобильными устройствами | Разрешает все операции в следующих функциональных областях:<br>• **Общие функции: Базовая функциональность.**<br>• **Управление мобильными устройствами: Общие.** |
| Оператор управления мобильными устройствами | Предоставляет права на **Чтение** и **Выполнение** в области **Общий функционал**: функциональная область **Базовая функциональность**.<br>Предоставляет права на **Чтение** и **Отправление только информационных команд на мобильные устройства** в следующих функциональных областях: **Управление мобильными устройствами**: функциональная область **Общие**. |
| Специалист по безопасности | Разрешает все операции в следующих функциональных областях: **Общий функционал**:<br>• **Доступ к объектам независимо от их списков ACL.**<br>• **Управление отчетами.**<br>Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой:** функциональная область **Подключения**.<br>Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации. |
| Пользователь Self Service Portal | Разрешает все операции в области **Управление мобильными устройствами**: Функциональная область **Self Service Portal**. Эта функция не поддерживается в версиях программы Kaspersky Security Center 11 и выше. |

| Роль | Описание |
|---|---|
| Контролер | Предоставляет права на **Чтение** в области **Общий функционал**: **Доступ к объектам независимо от их списков ACL** и **Общий функционал**: функциональная область **Управление отчетами**.<br>Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации. |
| Администратор Системного администрирования | Разрешает все операции в области **Общий функционал**: функциональные области **Базовая функциональность** и **Управление системой** (включая все функции). |
| Оператор Системного администрирования | Предоставляет права на **Чтение** и **Выполнение** (если применимо) в области **Общий функционал**: функциональные области **Базовая функциональность** и **Управление системой** (включая все функции). |

## См. также:

Сценарий: Настройка защиты сети .....400

## Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера (см. стр. 1192), вы можете настроить доступ к конкретным объектам, например, к требуемой задаче. Программа позволяет указать права доступа к следующим типам объектов:

- Группы администрирования
- Задачи
- Отчеты
- Выборки устройств
- Выборки событий

► *Чтобы назначить права доступа к конкретному объекту:*

1. В зависимости от типа объекта в главном меню перейдите в соответствующий раздел:
   - **Устройства → Иерархия групп**.
   - **Устройства → Задачи**.
   - **Мониторинг и отчеты → Отчеты**.
   - **Устройства → Выборки устройств**.
   - **Мониторинг и отчеты → Выборки событий**.
2. Откройте свойства объекта, к которому вы хотите настроить права доступа.

   Чтобы открыть окно свойств группы администрирования или задачи, нажмите на название объекта. Свойства других объектов можно открыть с помощью кнопки в панели инструментов.
3. В окне свойств откройте раздел **Права доступа**.

   Откроется список пользователей. Перечисленные пользователи и группы безопасности имеют права доступа к объекту. Если вы используете иерархию групп администрирования или Серверов, список и

права доступа по умолчанию наследуются от родительской группы администрирования или главного Сервера.

4. Чтобы иметь возможность изменять список, включите параметр **Использовать права пользователей**.
5. Настройте права доступа:
   - Используйте кнопки **Добавить** и **Удалить** для изменения списка.
   - Укажите права доступа для пользователя или группы безопасности. Выполните одно из следующих действий:
     - Если вы хотите указать права доступа вручную, выберите пользователя или группу безопасности, нажмите на кнопку **Права доступа** и укажите права доступа.
     - Если вы хотите назначить пользовательскую роль (см. стр. 1190)пользователю или группе безопасности, выберите пользователя или группу безопасности, нажмите на кнопку **Роли** и выберите роль для назначения.
6. Нажмите на кнопку **Сохранить**.

Права доступа к объекту настроены.

### См. также:



## Добавление учетной записи внутреннего пользователя

► *Чтобы добавить новую учетную запись пользователя Kaspersky Security Center:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новый объект** укажите параметры новой учетной записи пользователя:
   - Не меняйте указанное по умолчанию значение параметра **Пользователь**.
   - **Имя**.
   - **Пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A-Z);
       - нижний регистр (A-Z) (a-z);
       - числа (0-9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

Чтобы просмотреть введенный вами пароль, нажмите и удерживайте кнопку **Показать**.

> Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить максимальное количество попыток ввода пароля, как описано в разделе "Изменение количества попыток ввода пароля" (на стр. 768).
> Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.

- **Полное имя**
- **Описание**
- **Адрес электронной почты**
- **Телефон**

4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Созданная учетная запись пользователя отобразится в списке пользователей и групп пользователей.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Создание группы пользователей

► *Чтобы создать группу пользователей:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новый объект** выберите **Группа**.
4. Укажите следующие параметры группы пользователей:
   - **Имя группы**
   - **Описание**
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Созданная группа пользователей отобразится в списке пользователей и групп пользователей.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Изменение учетной записи внутреннего пользователя

► *Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.

3. В открывшемся окне на закладке **Общие** измените параметры учетной записи пользователя:
   - **Описание.**
   - **Полное имя.**
   - **Адрес электронной почты.**
   - **Основной телефон.**
   - **Пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A-Z);
       - нижний регистр (A-Z) (a-z);
       - числа (0-9);
       - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
     - Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

     Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

     Количество попыток ввода пароля пользователем ограничено. По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить (см. стр. 768) разрешенное количество попыток; однако из соображений безопасности не рекомендуется уменьшать это число. Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.
   - При необходимости переведите переключатель в положение **Выключен**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
4. На закладке **Дополнительные настройки безопасности** вы можете указать параметры безопасности для этой учетной записи.
5. На закладке **Группы** можно добавить пользователя или группу безопасности.
6. На закладке **Устройства** можно назначить устройства пользователю (см. стр. 1220).
7. На закладке **Роли** можно назначить роль пользователю (см. стр. 1223).
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей и групп безопасности.

## См. также:

Сценарий: Настройка защиты сети .....400

kaspersky

## Изменение группы пользователей

Можно изменять только внутренние группы.

► *Чтобы изменить группу пользователей:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Выберите группу пользователей, которую требуется изменить.
3. В открывшемся окне измените параметры группы пользователей:
   - **Имя**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная группа пользователей отобразится в списке пользователей и групп пользователей.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Добавление учетных записей пользователей во внутреннюю группу

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу.

► *Чтобы добавить учетные записи пользователей в группу:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу.
3. Нажмите на кнопку **Назначить группу**.
4. В открывшемся окне **Назначение группы** выберите группу, в которую требуется добавить учетные записи пользователей.
5. Нажмите на кнопку **Назначить**.

Учетные записи пользователей добавлены в группу.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств https://support.kaspersky.com/KESMob/10SP4MR3/ru-RU/214537.htm.

► *Чтобы назначить пользователя владельцем устройства:*

1. Если вы хотите назначить владельца устройства, подключенного к виртуальному Серверу администрирования, сначала переключитесь на виртуальный Сервер администрирования:
   a. В главном меню нажмите на значок шеврона ( ) справа от текущего имени Сервера администрирования.
   b. Выберите требуемый Сервер администрирования.
2. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**

   Откроется список пользователей. Если вы в данный момент подключены к виртуальному Серверу администрирования, в список входят пользователи текущего виртуального Сервера администрирования и главного Сервера администрирования.
3. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.
4. В открывшемся окне свойств пользователя перейдите на закладку **Устройства**.
5. Нажмите на кнопку **Добавить**.
6. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.
7. Нажмите на кнопку **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию: **Устройства** → **Управляемые устройства**, нажмите на имя устройства, которое вы хотите назначить, и перейдите по ссылке **Управление владельцем устройства**.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

► *Удаление пользователей или групп безопасности:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Пользователь или группа безопасности удалены.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Создание роли пользователя

► *Чтобы создать роль пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:
   - На закладке **Общие** измените имя роли.

     Нельзя изменять имена типовых ролей.
   - На закладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью (см. стр. 1223).
   - На закладке **Права доступа** измените права доступа к программам "Лаборатории и Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Изменение роли пользователя

► *Чтобы изменить роль пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На закладке **Общие** измените имя роли.

     Нельзя изменять имена типовых ролей.
   - На закладке **Параметры** измените область действия роли (см. стр. 1223), а также политики и профили политик, связанные с ролью.
   - На закладке **Права доступа** измените права доступа к программам "Лаборатории и Касперского".
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

### См. также:

Сценарий: Настройка защиты сети ..... 400

kaspersky

## Изменение области для роли пользователя

*Область роли пользователя* – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

► *Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:*

► *Способ 1:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Установите флажки напротив имен пользователей и групп безопасности, которые требуется добавить в область роли.
3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На странице **Выбор роли** в мастере выберите роль, которую требуется назначить.
5. На странице **Определение области** в мастере выберите группу администрирования, которую требуется добавить в область роли.
6. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

► *Способ 2:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, для которой требуется задать область.
3. В открывшемся окне свойств роли перейдите на закладку **Параметры**.
4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На странице **Определение области** в мастере выберите группу администрирования, которую требуется добавить в область роли.
6. На странице **Выбор пользователей** в мастере выберите пользователей и группы пользователей, которые требуется добавить в область роли.
7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.
8. Закройте окно свойств роли.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

### См. также:

Сценарий: Настройка защиты сети .....400

## Удаление роли пользователя

► *Чтобы удалить роль пользователя:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Установите флажок напротив роли, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Роль пользователя будет удалена.

### См. также:

Сценарий: Настройка защиты сети .....400

## Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск программ городской навигации для всех устройств группы администрирования. Программы городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" (см. стр. 1190) владельцу этого устройства и создать профиль политики, разрешающий использовать программы городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать программы городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать программы городской навигации на устройстве, принадлежащем вашей организации. Однако использование программ городской навигации будет запрещено на других устройствах этой группы администрирования.

► *Чтобы связать роль с профилем политики:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на закладке **Общие**.
3. Перейдите на закладку **Параметры** и прокрутите страницу вниз до раздела **Политики и профили политик**.
4. Нажмите на кнопку **Изменить**.
5. Чтобы связать роль с:
   - **Существующим профилем политики** – нажмите на значок (>) рядом с именем требуемой политики, а затем установите флажок рядом с профилем политики, с которым вы хотите связать роль.
   - **Новым профилем политики**:
     a. Установите флажок около политики, для которой вы хотите создать профиль политики.
     b. Нажмите на кнопку **Создать профиль**.

c. Укажите имя нового профиля политики и настройте параметры профиля политики.

d. Нажмите на кнопку **Сохранить**.

e. Установите флажок рядом с новым профилем политики.

6. Нажмите на кнопку **Назначить роль**.

Выбранный профиль политики связывается с ролью и появляется в свойствах роли. Профиль автоматически применяется ко всем устройствам, владельцам которых назначена эта роль.

### См. также:

Сценарий: Настройка защиты сети .....400

## Работа с объектами в Kaspersky Security Center 14.2 Web Console

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия.* Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- Серверы администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать объект с выбранной ревизией другого однотипного объекта;
- просматривать выбранную ревизию;
- откатывать изменения объекта к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- номер ревизии объекта;
- дата и время изменения объекта;
- имя пользователя, изменившего объект;
- выполненное действие с объектом;
- описание ревизии изменения параметров объекта.

По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Описание**. В окне **Описание ревизии объекта** введите текст описания ревизии.

## Добавление описания ревизии

Kaspersky Security Center позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается ревизия. Каждая ревизия имеет номер.

Вы можете добавить описание для ревизии, чтобы в дальнейшем было проще найти необходимую ревизию в списке.

► *Чтобы добавить описание ревизии:*

1. Перейдите к разделу **История ревизий** объекта (см. стр. 1225).
2. В списке ревизий объекта выберите ревизию, для которой нужно добавить описание.
3. Нажмите на кнопку **Изменить описание**.

   Откроется окно **Описание**.
4. В окне **Описание** введите текст описания ревизии.

   По умолчанию описание ревизии объекта не заполнено.
5. Нажмите на кнопку **Сохранить**.

Описание добавлено для ревизии объекта.

## Удаление объектов

В этом разделе описано, как удалять объекты и просматривать информацию объектов после того, как они были удалены.

Вы можете удалять следующие объекты:

- политики;
- задачи;
- инсталляционные пакеты;
- виртуальные Серверы администрирования;
- пользователей;
- группы пользователей;
- группы администрирования.

Когда вы удаляете объект, информация об этом записывается в базу данных. Срок хранения (на стр. 814) информации удаленных объектов такой же, как и срок хранения ревизий объектов (рекомендуемый срок 90 дней). Можно изменить время хранения только при наличии права на **Изменение** (на стр. 798) для области **Удаленные объекты**.

**Об удалении клиентских устройств**

При удалении управляемого устройства из группы администрирования программа перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные программы "Лаборатории Касперского" – Агент администрирования и программа безопасности, например Kaspersky Endpoint Security (если есть) – остаются на устройстве.

Kaspersky Security Center Cloud Console обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств (на стр. 1126) и устройство соответствует критериям правила перемещения, оно автоматически перемещается в группу администрирования в соответствии с правилом.
- Устройство сохраняется в группе Нераспределенные устройства и автоматически удаляется из группы в соответствии с правилами хранения устройств (на стр. 1063).

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования. Такие устройства не удаляются автоматически, вы можете сделать это только вручную. Если вам нужно удалить устройство с зашифрованным диском, сначала расшифруйте диск, а затем удалите устройство.
  При удалении устройства с зашифрованным диском данные, необходимые для расшифровки диска, также удаляются. В этом случае вы сможете расшифровать диск только в том случае, если у пользователя устройства есть пароль на расшифровку и на устройстве все еще установлена программа безопасности, которая использовалась для шифрования диска, например Kaspersky Endpoint Security для Windows.

При удалении устройства из группы Нераспределенные устройства вручную программа удаляет устройство из списка. После удаления устройства, установленные программы "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети (на стр. 325), Kaspersky Security Center обнаружит устройство во время опроса сети и снова добавит его в группу Нераспределенные устройства. Поэтому удалять устройство вручную целесообразно только в том случае, если оно невидимо для Сервера администрирования.

### См. также:

Удаление объекта.....817

# Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

kaspersky

## В этом разделе



## О KSN

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. KSN позволяет получать из репутационных баз "Лаборатории Касперского" информацию о программах, установленных на управляемых устройствах.

Kaspersky Security Center поддерживает следующие инфраструктурные решения KSN:

- *Глобальный KSN* – решение, позволяющее обмениваться информацией с Kaspersky Security Network. Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе программ "Лаборатории Касперского", установленных на клиентских устройствах, находящихся под управлением Kaspersky Security Center. Передача информации выполняется в соответствии с настроенными параметрами доступа к KSN (см. стр. 830). Специалисты "Лаборатории Касперского" дополнительно анализируют полученную информацию и включают ее в репутационные и статистические базы данных Kaspersky Security Network. Kaspersky Security Center использует это решение по умолчанию.
- *Локальный KSN* – это решение, которое предоставляет пользователям устройств с установленными программами "Лаборатории Касперского" доступ к базам данных Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в KSN. Kaspersky Private Security Network (Локальный KSN) предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:
  - Устройства пользователей не подключены к интернету.
  - Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

  Вы можете настроить параметры доступа (см. стр. 830) Kaspersky Private Security Network в разделе **Параметры KSN прокси-сервера** окна свойств Сервера администрирования.

Программа предлагает присоединиться к KSN во время работы мастера первоначальной настройки. Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. стр. 832).

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с предыдущей версией Положения о KSN, которую вы приняли ранее.

Когда KSN включен, Kaspersky Security Center проверяет доступность серверов KSN. Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871). Это необходимо, чтобы убедиться, что уровень безопасности поддерживается для управляемых устройств.

Клиентские устройства, находящиеся под управлением Сервера администрирования, взаимодействуют с KSN при помощи службы прокси-сервера KSN. Служба прокси-сервера KSN предоставляет следующие возможности:

- Клиентские устройства могут выполнять запросы к KSN и передавать в KSN информацию, даже если они не имеют прямого доступа в интернет.
- Прокси-сервер KSN кеширует обработанные данные, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентским устройством запрошенной информации.

Вы можете настроить параметры прокси-сервера KSN в разделе **Прокси-сервер KSN** окна свойств Сервера администрирования (см. стр. 830).

## Настройка доступа к KSN

Можно задать доступ к Kaspersky Security Network (KSN) с Сервера администрирования и с точки распространения.

► *Чтобы настроить доступ Сервера администрирования к Kaspersky Security Network:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования [Включено]**.

   Передача данных от клиентских устройств в KSN регулируется политикой Kaspersky Endpoint Security, действующей на клиентских устройствах. Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

4. Переведите переключатель в положение **Использовать Kaspersky Security Network [Включено]**.

   Если параметр включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". При включении этого параметра убедитесь, что вы прочитали и принимаете условия Положения о KSN.

   Если вы используете Локальный KSN, установите флажок **Использовать Kaspersky Private Security Network [Включено]** и по кнопке **Файл с параметрами прокси-сервера KSN** загрузите параметры Локального KSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами Локального KSN.

При включении Локального KSN обратите внимание на точки распространения настроенные на отправление KSN запросов напрямую облачной-службе KSN. Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к облачной-службе KSN. Чтобы перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения. Вы можете включить этот параметр в свойствах точки распространения или политики Агента администрирования.

При переводе переключателя в положение **Использовать Kaspersky Private Security Network [Включено]** появится сообщение с подробной информацией о Локальном KSN.

Работу с Локальным KSN поддерживают следующие программы "Лаборатории Касперского":

- Kaspersky Security Center;
- Kaspersky Endpoint Security для Windows;
- Kaspersky Endpoint Security для Linux;
- Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2;
- Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент.

Если вы включите Локальный KSN в Kaspersky Security Center, эти программы получат об этом информацию о поддержке Локального KSN. В окне свойств программы в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается **Поставщик KSN: Локальный KSN**. В противном случае отображается **Поставщик KSN: Глобальный KSN**.

Если для работы с Локальным KSN вы используете версии программ ниже Kaspersky Security для виртуальных сред 3.0 Защита без агента Service Pack 2 или ниже Kaspersky Security для виртуальных сред 3.0 Service Pack 1 Легкий агент, рекомендуется использовать подчиненные Серверы администрирования, для которых не настроено использование Локального KSN.
Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен Локальный KSN в окне свойств Сервера администрирования в разделе **Параметры прокси-сервера KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к Локальному KSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали Локальный KSN напрямую. В противном случае запрос от управляемой программы не будет передан в Локальный KSN.
6. Настройте параметры подключения Сервера администрирования к службе прокси-сервера KSN:
   - В блоке **Параметры подключения**, в поле ввода **TCP-порт** укажите номер TCP-порта, через который будет выполняться подключение к прокси-серверу KSN. По умолчанию подключение к прокси-серверу KSN выполняется через порт 13111.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **UDP-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.
7. Переведите переключатель в положение **Подключать подчиненные Серверы администрирования к KSN через главный Сервер [Включено]**.

   Если этот параметр включен, подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера KSN. Если этот параметр выключен,

подчиненные Серверы администрирования подключаются к KSN самостоятельно. В этом случае управляемые устройства используют подчиненные Серверы администрирования как прокси-серверы KSN.

> Подчиненные Серверы администрирования используют главный Сервер администрирования в качестве прокси-сервера, если в свойствах подчиненных Серверов администрирования в разделе **Параметры прокси-сервера KSN** также переключатель переведен в положение **Включить прокси-сервер KSN на Сервере администрирования [Включено]**.

8. Нажмите на кнопку **Сохранить**.

В результате параметры доступа к KSN будут сохранены.

Можно также настроить доступ к KSN со стороны точки распространения, например, если необходимо снизить нагрузку на Сервер администрирования. Точка распространения, выполняющая роль прокси-сервера KSN, отправляет KSN запросы от управляемых устройств напрямую в "Лабораторию Касперского", минуя Сервер администрирования.

► *Чтобы настроить доступ точки распространения к Kaspersky Security Network (KSN):*

1. Убедитесь, что точка распространения была назначена вручную (см. стр. 1266).
2. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На закладке **Общие** выберите раздел **Точки распространения**.
4. Нажмите на имя точки распространения, чтобы открыть окно ее свойств.
5. В окне свойств точки распространения в разделе KSN, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN / Локальному KSN непосредственно через интернет**.
6. Нажмите на кнопку **ОК**.

Точка распространения будет исполнять роль прокси-сервера KSN.

## Включение и отключение KSN

► *Чтобы включить KSN:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования [Включено]**.

   В результате будет включена служба прокси-сервера KSN.
4. Переведите переключатель в положение **Использовать Kaspersky Security Network [Включено]**.

   В результате KSN будет включен.

Если переключатель включен, клиентские устройства будут передавать результаты установки патчей в "Лабораторию Касперского". Включая переключатель, вы должны прочитать и принять условия Положения о KSN.

5. Нажмите на кнопку **Сохранить**.

► *Чтобы выключить KSN:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Переведите переключатель в положение **Включить прокси-сервер KSN на Сервере администрирования [Выключено]**, чтобы отключить службу прокси-сервера KSN, или переключите переключатель в положение **Использовать Kaspersky Security Network [Выключено]**.

   Если переключатель выключен, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

   Если вы используете Локальный KSN, переведите переключатель в положение**Использовать Private Kaspersky Security Network [Выключено]**.

   В результате KSN будет выключен.

4. Нажмите на кнопку **Сохранить**.

## Просмотр принятого Положения о KSN

При включении Kaspersky Security Network (KSN) вы должны прочитать и принять Положение о KSN. Вы можете просмотреть принятое Положение о KSN в любое время.

► *Чтобы просмотреть принятое Положение о KSN:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Перейдите по ссылке **Просмотреть Положение о Kaspersky Security Network**.

В открывшемся окне вы можете просмотреть текст принятого Положения о KSN.

## Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN (на стр. 1232), которое вы читаете и принимаете при включении KSN. Если Положение о KSN обновлено, оно отображается при обновлении Сервера администрирования или при обновлении Сервера администрирования с предыдущей версии. Вы можете принять обновленное Положение о KSN или отклонить его. Если вы отклоните его, вы продолжите использовать KSN в соответствии с версией Положения о KSN, которую вы приняли ранее.

После обновления Сервера администрирования или после обновления с предыдущей версии Сервера администрирования, обновленное Положение о KSN отображается автоматически. Если вы отклоните обновленное Положение о KSN, вы все равно сможете просмотреть и принять его позже.

► *Чтобы просмотреть и принять или отклонить обновленное Положение о KSN:*

1. Перейдите по ссылке **Просмотреть уведомления о событиях** в правом верхнем углу главного окна программы.

   Откроется окно **Уведомления**.

2. Перейдите по ссылке **Просмотреть обновленное Положение о KSN**.

   Откроется окно **Обновленное Положение о Kaspersky Security Network**.

3. Прочтите Положение о KSN, а затем примите решение, нажав одну из следующих кнопок:

   - **Я принимаю условия обновленного Положения о KSN**
   - **Использовать KSN со старым Положением о KSN**

В зависимости от вашего выбора KSN продолжит работу в соответствии с условиями текущего или обновленного Положения о KSN. Вы можете в любой момент просмотреть текст принятого Положения о KSN (на стр. 1232) в свойствах Сервера администрирования.

## Проверка, работает ли точка распространения как прокси-сервер KSN

На управляемом устройстве, которое выполняет роль точки распространения, вы можете включить прокси-сервер KSN. Управляемое устройство работает как прокси-сервер KSN, если на нем запущена служба ksnproxy. Вы можете проверить включить или выключить эту службу на устройстве локально.

Вы можете назначить устройство с операционной системой Windows или Linux в качестве точки распространения. Способ проверки точки распространения зависит от операционной системы этой точки распространения.

► *Чтобы проверить, работает ли точка распространения с операционной системой Windows как прокси-сервер KSN:*

1. На устройстве, которое выполняет роль точки распространения, в Windows откройте окно **Службы** (**Все программы** → **Администрирование** → **Службы**).
2. В списке служб проверьте, запущена ли служба прокси-сервера KSN – ksnproxy.

   Если служба ksnproxy запущена, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN Proxy для управляемых устройств, входящих в область действия точки распространения.

При необходимости службу ksnproxy можно выключить. В этом случае Агент администрирования на точке распространения больше не участвует в Kaspersky Security Network. Для этого требуются права локального администратора.

► *Чтобы проверить, работает ли точка распространения с операционной системой Linux как прокси-сервер KSN:*

1. На устройстве, выполняющем роль точки распространения, отобразится список запущенных процессов.
2. В списке запущенных процессов проверьте запущен ли процесс `/opt/kaspersky/ksc64/sbin/ksnproxy`.

Если процесс `/opt/kaspersky/ksc64/sbin/ksnproxy` запущен, то Агент администрирования на устройстве участвует в Kaspersky Security Network и работает как прокси-сервер KSN для управляемых устройств, входящих в область действия точки распространения.

# Обновление баз и программ "Лаборатории Касперского"

Установка обновлений исполняемых программных модулей программ «Лаборатории Касперского», не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программ из безопасного состояния.

В этом разделе описаны шаги, которые вы должны выполнить для регулярных обновлений:

- баз и программных модулей "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

## В этом разделе



## Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, программных модулей и программ "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации (см. стр. 400), вы должны поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и программных модулей "Лаборатории Касперского";

- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программы безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

**Предварительные требования**

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, программных модулей и программ "Лаборатории Касперского" вручную (см. стр. 1262) или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты программы безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14.2 Web Console (см. стр. 1035).
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. стр. 400).
3. Назначено соответствующее количество точек распространения (см. стр. 167) в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и программ "Лаборатории Касперского" состоит из следующих этапов:

a. **Выбор схемы обновления**

   Существует несколько схем (см. стр. 453), которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и программ безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

b. **Создание задачи для загрузки обновлений в хранилище Сервера администрирования**

   Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, создайте задачу сейчас.

   Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования, а также обновления баз и программных модулей для Kaspersky Security Center. После загрузки обновлений их можно распространять на управляемые устройства.

   Если в вашей сети назначены точки распространения, обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. В этом случае управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.

   Инструкции:

   Консоль администрирования: Создание задачи загрузки обновлений в хранилище Сервера администрирования (см. стр. 461).

   Kaspersky Security Center 14.2 Web Console: Создание задачи загрузки обновлений в хранилище Сервера администрирования (см. стр. 1244).

c. **Создание задачи загрузки обновлений в хранилища точек распространения (если требуется)**

   По умолчанию обновления загружаются в хранилища точек распространения из хранилища Сервера администрирования. Вы можете настроить Kaspersky Security Center так, чтобы точки

распространения загружали обновления непосредственно с серверов обновлений "Лаборатории Касперского". Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Когда вашей сети назначены точки распространения и создана задача *Загрузка обновлений в хранилища точек распространения*, точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Инструкции:

Консоль администрирования: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. 465).

Kaspersky Security Center 14.2 Web Console: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. 1252).

**d. Настройка точек распространения**

Если в вашей сети назначены точки распространения(см. стр. 481), убедитесь, что параметр **Распространять обновления** включен в свойствах всех требуемых точек распространения. Если этот параметр выключен для точки распространения, устройства, включенные в область действия точки распространения, загружают обновления из хранилища Сервера администрирования.

Если вы хотите, чтобы управляемые устройства получали обновления только от точек распространения, включите параметр **Распространять файлы только через точки распространения** в политике Агента администрирования (см. стр. 750).

**e. Оптимизация процесса обновления с использованием офлайн-модели получения обновлений или загрузки файлов различий (если требуется)**

Вы можете оптимизировать процесс обновления, используя офлайн-модель загрузки обновлений (см. стр. 474) (включена по умолчанию), или используя файлы различий (см. стр. 459). Для каждого сегмента сети вы должны выбрать, какую из этих двух функций включить, так как они не могут работать одновременно.

Когда офлайн-модель получения обновлений включена, Агент администрирования загружает необходимые обновления на управляемое устройство после загрузки обновлений в хранилище Сервера администрирования, прежде чем программа безопасности запросит обновления. Это повышает надежность процесса обновления. Чтобы использовать эту функцию, установите флажок **Загружать обновления и антивирусные базы с Сервера администрирования заранее** в свойствах политики Агента администрирования (см. стр. 750).

Если вы не используете офлайн-модель загрузки обновлений, вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами, используя файлы различий. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или программных модулей "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкции:

Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского" (см. стр. 459).

Консоль администрирования: Включение и выключение офлайн-модели получения обновлений (см. стр. 476).

Kaspersky Security Center 14.2 Web Console: Включение и выключение офлайн-модели получения обновлений (см. стр. 1261).

**f. Проверка полученных обновлений (если требуется)**

Перед установкой загруженных обновлений вы можете проверить обновления с помощью задачи *Проверка обновлений*. Эта задача последовательно запускает задачи обновления устройства и задачи поиска вредоносного ПО, настроенные с помощью параметров для указанного набора тестовых устройств. После получения результатов задачи Сервер администрирования запустит или заблокирует распространение обновлений на оставшиеся устройства.

Задача *Проверка обновлений* может быть выполнена как часть задачи *Загрузка обновлений в хранилище Сервера администрирования*. В свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* включите параметр **Выполнять проверку обновлений перед распространением** в Консоли администрирования или параметр **Выполнить проверку обновлений** в Kaspersky Security Center 14.2 Web Console.

Инструкции:

Консоль администрирования: Проверка полученных обновлений (см. стр. 470).

Kaspersky Security Center 14.2 Web Console: Проверка обновлений (см. стр. 1250).

**g. Одобрение и отклонение обновлений программного обеспечения**

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Неопределенные обновления могут быть установлены только на Агенте администрирования и других компонентах Kaspersky Security Center (см. стр. 476) в соответствии с параметрами политики Агента администрирования. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для программы безопасности было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств. Обновления для компонентов Kaspersky Security Center не могут быть удалены.

Инструкции:

Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (см. стр. 493).

Kaspersky Security Center 14.2 Web Console: Одобрение и отклонение обновлений программного обеспечения (см. стр. 1259).

**h. Настройка автоматической установки обновлений и патчей для компонентов Kaspersky Security Center**

Загруженные обновления и патчи для Агента администрирования и других компонентов Kaspersky Security Center (см. стр. 476) устанавливаются автоматически. Если вы оставили включенным параметр **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** в свойствах Агента администрирования, тогда все обновления будут установлены автоматически после их загрузки в хранилище (или несколько хранилищ). Если параметр выключен, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.

Инструкции:

Консоль администрирования: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 477).

Kaspersky Security Center 14.2 Web Console: Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 1256).

**i. Установка обновлений для Сервера администрирования**

Обновления программного обеспечения для Сервера администрирования не зависят от статусов обновлений. Они не устанавливаются автоматически и должны быть предварительно одобрены администратором на закладке **Мониторинг** в Консоли администрирования (**Сервер администрирования** `<имя Сервера>` → **Мониторинг**) или на закладке **Уведомления** в Kaspersky

Security Center 14.2 Web Console (**Мониторинг и отчеты** → **Уведомления**). После этого администратор должен явно запустить установку обновлений.

j. **Настройка автоматической установки обновлений для программ безопасности**

Создайте задачу *Обновление* для управляемых программ, чтобы обеспечить своевременное обновление программ, программных модулей и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище** (см. стр. 1112).

Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять программы безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования (версии 13.2 или выше) и Агент администрирования (версии 13.2 или выше).

По умолчанию обновления для Kaspersky Endpoint Security для Windows и для Kaspersky Endpoint Security для Linux устанавливаются только после изменения статуса обновления на *Одобрено*. Вы можете изменить параметры обновления в задаче *Обновление*.

Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

Инструкции:

Консоль администрирования: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (см. стр. 473).

Kaspersky Security Center 14.2 Web Console: Автоматическая установка обновлений для Kaspersky Endpoint Security на устройства (см. стр. 1257).

**Результаты**

По завершении сценария Kaspersky Security Center настроен для обновления баз "Лаборатории Касперского" и установленных программ "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования или в хранилища точек распространения. Теперь вы можете приступить к мониторингу состояния сети.

## См. также:

Сценарий: Настройка защиты сети ..... 400

# Об обновлении баз, программных модулей и программ "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вы должны своевременно предоставлять обновления следующего:

- баз и программных модулей "Лаборатории Касперского";

Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и программных модулей "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, программа использует публичные DNS-серверы (см. стр. 871). Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

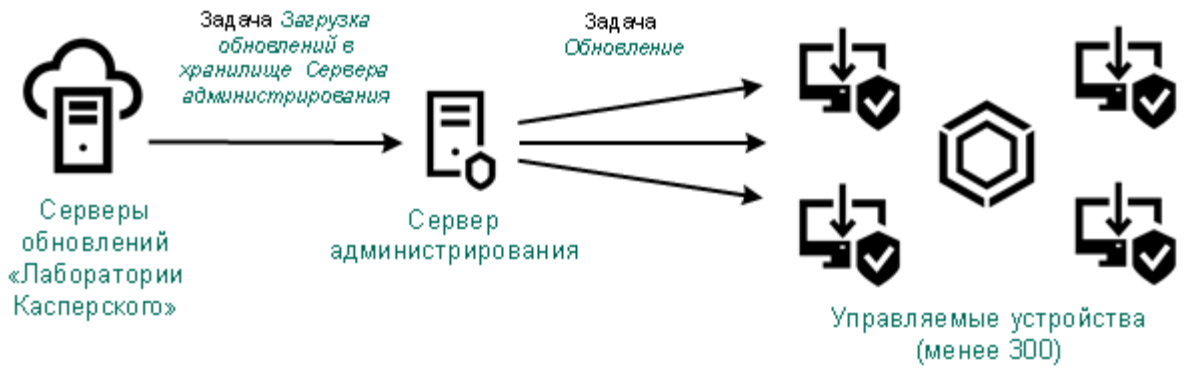
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования.*
- С помощью двух задач:
  - задачи *Загружать обновления в хранилище Сервера администрирования*;
  - задачи *Загружать обновления в хранилища точек распространения*.
- Вручную через локальную папку, общую папку или FTP-сервер
- Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах
- Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

**Использование задачи Загрузка обновлений в хранилище Сервера администрирования**

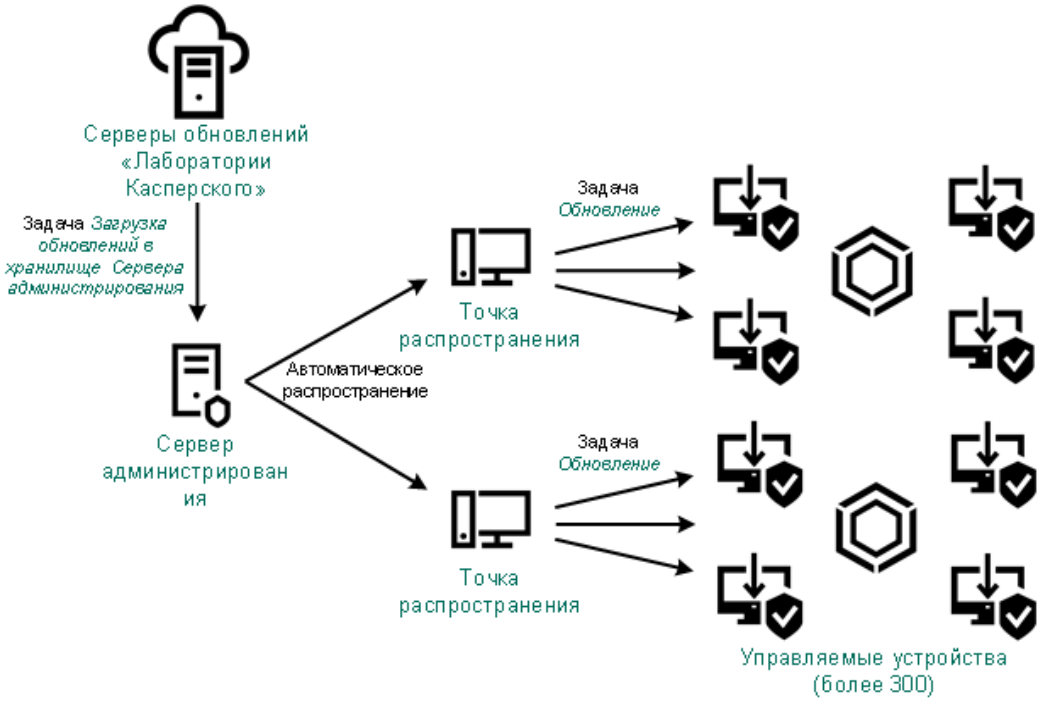
В этой схеме Kaspersky Security Center загружает обновления с помощью задачи *Загружать обновления в хранилище Сервера администрирования*. В небольших сетях, которые содержат менее 300 управляемых устройств в одном сегменте сети или менее десяти управляемых устройств в каждом сегменте, обновления распространяются на управляемые устройства непосредственно из хранилища Сервера администрирования (см. рисунок ниже).




По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

Если ваша сеть содержит более 300 управляемых устройств в одном сегменте сети или ваша сеть содержит несколько сегментов, в которых больше девяти управляемых устройств, мы рекомендуем использовать точки распространения (см. стр. 167) для распространения обновлений на управляемые устройства (см. рисунок ниже). Точки распространения уменьшают загрузку Сервера администрирования и оптимизируют трафик между Сервером администрирования и управляемыми устройствами. Вы можете рассчитать (см. стр. 167) количество точек распространения и их конфигурацию, необходимые для вашей сети.

В этой схеме обновления автоматически загружаются из хранилища Сервера администрирования в хранилища точек распространения. Управляемые устройства, входящие в область действия точки распространения, загружают обновления из хранилищ точек распространения, вместо хранилища Сервера администрирования.




После завершения задачи *Загружать обновления в хранилище Сервера администрирования* следующие обновления загружаются в хранилище Сервера администрирования:

- Базы и программные модули "Лаборатории Касперского" для Kaspersky Security Center.

  Эти обновления устанавливаются автоматически.

- Базы и программные модули "Лаборатории Касперского" для программ безопасности на управляемых устройствах.

  Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Windows (см. стр. 1257) .

- Обновления для Сервера администрирования.

  Эти обновления не устанавливаются автоматически. Администратор должен явно одобрить обновления и запустить установку обновлений.

  > Для установки патчей на Сервере администрирования требуются права локального администратора.

- Обновления для компонентов Kaspersky Security Center.

  По умолчанию эти обновления устанавливаются автоматически. Вы можете изменить параметры политики Агента администрирования (см. стр. 1256) .

- Обновления для программ безопасности.

  По умолчанию программа Kaspersky Endpoint Security для Windows устанавливает только те обновления, которые вы одобрили. (Вы можете одобрить обновления с помощью Консоли администрирования или  (см. стр. 493) Kaspersky Security Center 14.2 Web Console (см. стр. 1259)). Обновления устанавливаются с помощью задачи *Обновление* и могут быть настроены в свойствах этой задачи.

Задача *Загрузка обновлений в хранилище Сервера администрирования* недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

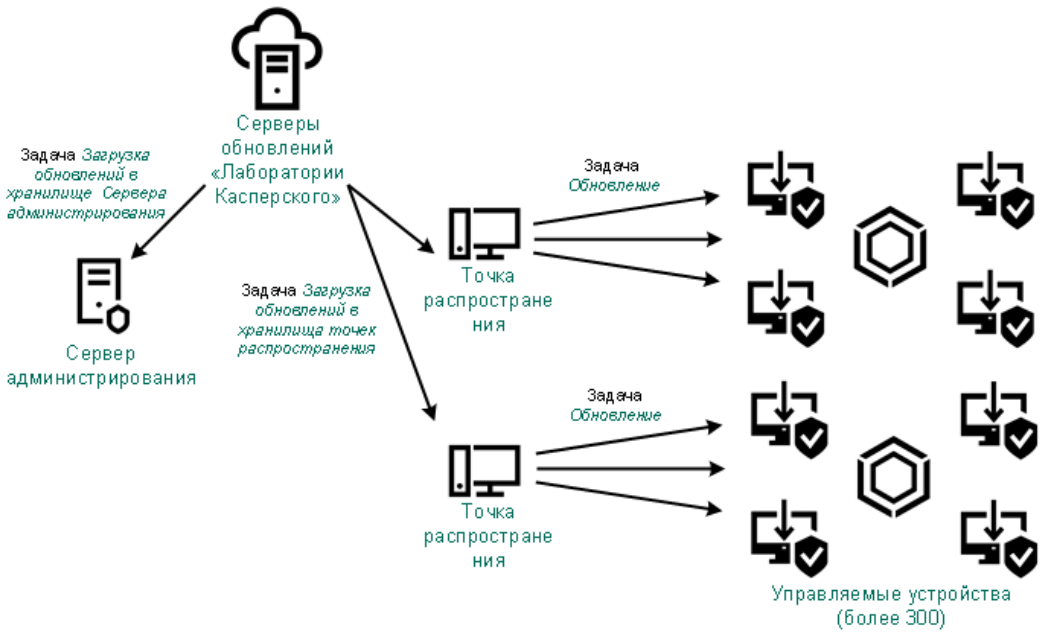
Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются программами. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загружать обновления в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и программных модулей "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия программы;
- идентификатор установки программы;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

**Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения**

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.




По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и / или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загружать обновления в хранилища точек распространения* в дополнение к задаче *Загружать обновления в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

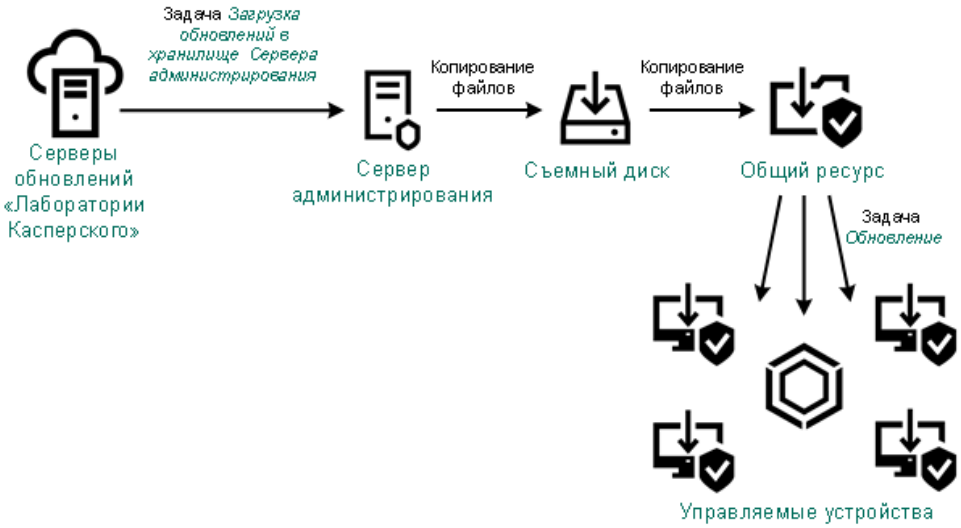
Точки распространения под управлением macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского".

Если устройства с операционной системой macOS находятся в области действия задачи *Загрузка обновлений в хранилища точек распространения*, задача завершится со статусом *Сбой*, даже если она успешно завершилась на всех устройствах с операционной системой Windows.

Для этой схемы также требуется задача *Загружать обновления в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и программных модулей "Лаборатории Касперского" для Kaspersky Security Center.

**Вручную через локальную папку, общую папку или FTP-сервер**

Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, программных модулей и программ "Лаборатории Касперского" (см. стр. 1262) . В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в настройках Kaspersky Endpoint Security (см. рисунок ниже).

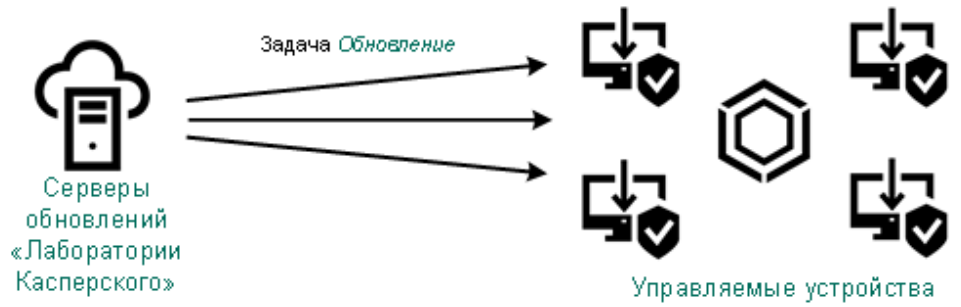



Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих онлайн-справках:

- Онлайн-справка Kaspersky Endpoint Security для Windows.
- Онлайн-справка Kaspersky Endpoint Security для Linux.

**Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security на управляемых устройствах**

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).




В этой схеме программы безопасности не используют хранилища, предоставленные Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в интерфейсе программы безопасности. Дополнительную информацию об этих параметрах см. в следующих онлайн-справках:

- Онлайн-справка Kaspersky Endpoint Security для Windows
- Онлайн-справка Kaspersky Endpoint Security для Linux

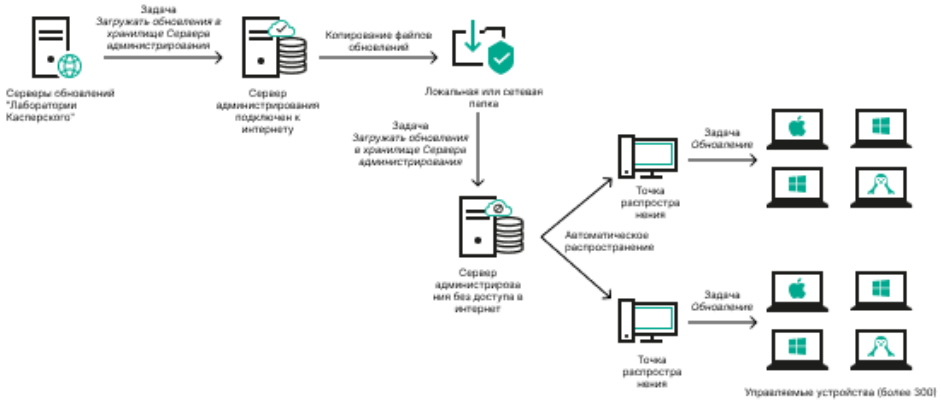
**Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет**

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузить обновления в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются программами безопасности, наборы программ безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 1244), а затем включите параметр **Загружать обновления, используя старую схему**.




- Kaspersky Update Utility https://support.kaspersky.ru/updater4

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера* (см. стр. 1244), а затем включите параметр **Загружать обновления, используя старую схему**.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

# Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загружать обновления в хранилище Сервера администрирования* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Задача *Загружать обновления в хранилище Сервера администрирования* может быть создана в одном экземпляре. Поэтому вы можете создать задачу *Загружать обновления в хранилище Сервера администрирования* только в случае, если она была удалена из списка задач Сервера администрирования.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования. Список обновлений включает:

- обновления баз и программных модулей для Сервера администрирования;
- обновления баз и программных модулей для программ "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления программ безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений* (см. стр. 1250). Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить их перед распространением, настройте параметр **Выполнить проверку обновлений** в параметрах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

► *Чтобы создать задачу **Загружать обновления в хранилище Сервера администрирования**:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для программы Kaspersky Security Center выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Запустить**.

   Задача будет создана и отобразится в списке задач.
7. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
8. В окне свойств задачи на закладке **Параметры программы** укажите следующие параметры:

   - **Источники обновлений**

В качестве источника обновлений для Сервера администрирования могут быть использованы следующие ресурсы:

- Источники обновлений

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы. По умолчанию Сервер администрирования взаимодействует с серверами обновлений "Лаборатории Касперского" и загружает обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования на использование протокола HTTP вместо HTTPS.

  Выбрано по умолчанию.
- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует

аутентификации, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

Если общая папка с обновлениями защищена паролем, включите параметр **Задать учетную запись для доступа к общей папке источника обновлений (если используется)** и введите учетные данные, необходимые для доступа.

- **Папка для хранения обновлений**
- Прочие параметры:
  - **Принудительно обновить подчиненные Серверы**

    Если флажок установлен, после получения обновлений Сервер администрирования будет запускать задачи получения обновлений подчиненными Серверами администрирования. В противном случае задачи обновления на подчиненных Серверах администрирования начинаются в соответствии с расписанием.

    По умолчанию параметр выключен.
  - **Копировать полученные обновления в дополнительные папки**

Если флажок установлен, после получения обновлений Сервер администрирования будет копировать обновления в указанные папки. Используйте этот параметр, если хотите управлять вручную обновлениями на вашем устройстве.

Например, вы можете использовать этот параметр в следующей ситуации: сеть организации содержит несколько независимых подсетей и устройства из каждой подсети не имеют доступ к другой подсети. При этом устройства во всех подсетях имеют доступ к общей сетевой папке. В этом случае для Сервера администрирования в одной из подсетей укажите загрузку обновлений с серверов обновлений "Лаборатории Касперского", включите этот параметр и укажите эту сетевую папку. В задаче загрузка обновлений в хранилище для Сервера администрирования укажите эту же сетевую папку в качестве источника обновлений.

По умолчанию параметр выключен.

- **Не обновлять устройства и подчиненные Серверы администрирования принудительно до окончания копирования**

  Если флажок установлен, задачи получения обновлений клиентскими устройствами и подчиненными Серверами администрирования будут запускаться после окончания копирования обновлений из сетевой папки обновлений в дополнительные папки обновлений.

  Этот флажок должен быть установлен, если клиентские устройства и подчиненные Серверы администрирования скачивают обновления из дополнительных сетевых папок.

  По умолчанию параметр выключен.

- **Состав обновлений**
  - **Загрузить файлы различий**

    Этот параметр включает функцию загрузки файлов различий (см. стр. 459).

    По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**
- **Выполнить проверку обновлений**

Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу (см. стр. 1250) проверки обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

По умолчанию параметр выключен.

1. В окне свойств задачи на закладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию:**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят

на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то

задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить, если задача выполняется дольше (мин)**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

2. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

В результате выполнения задачи *Загружать обновления в хранилище Сервера администрирования* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

### См. также:



## Проверка полученных обновлений

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загружать обновления в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты программы безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования (см. стр. 1124) с несколькими тестовыми устройствами. Эта группа понадобится вам для проверки обновлений.

   В качестве тестовых устройств рекомендуется использовать хорошо защищенные устройства с наиболее распространенной в сети организации программной конфигурацией. Такой подход повышает качество и вероятность обнаружения вирусов при проверке, а также минимизирует риск ложных срабатываний. При нахождении вирусов на тестовых устройствах задача *Проверка обновлений* считается завершившейся неудачно.

2. Создайте задачи обновления и поиска вредоносного ПО (см. стр. 1111) для какой-нибудь программы, которую поддерживает Kaspersky Security Center, например,Kaspersky Endpoint Security для Windows или Kaspersky Security для Windows Server. При создании задач обновления и поиска вредоносного ПО укажите группу администрирования с тестовыми устройствами.

Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вредоносного ПО на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вредоносного ПО.

3. Использование задачи *Загружать обновления в хранилище Сервера администрирования* (см. стр. 1244).

► *Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:*

1. В главном окне программы перейдите к закладке **Устройства → Задачи**.
2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на закладку **Параметры программы** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выбрать задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.
5. Если вы не создавали задачу *Проверка обновлений* ранее:
   a. Нажмите на кнопку **Новая задача**.
   b. В открывшемся мастере создания задачи укажите имя задачи, если вы хотите изменить предустановленное имя.
   c. Выберите созданную ранее группу администрирования с тестовыми устройствами.
   d. Выберите задачу обновления нужной программы, поддерживаемой Kaspersky Security Center, а затем выберите задачу поиска вредоносного ПО.

      После этого появляются следующие параметры. Рекомендуется оставить их включенными:

      - **Перезагружать устройство после обновления баз**
      - **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

   e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.
6. Закройте окно свойств задачи *Загружать обновления в хранилище Сервера администрирования*, нажав на кнопку**ОК**.

Автоматическая проверка обновлений включена. Теперь можно запустить задачу *Загружать обновления в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

kaspersky

# Создание задачи загрузки обновлений в хранилища точек распространения

Задача *Загрузка обновлений в хранилища точек распространения* работает только с точками распространения под управлением Windows. Точки распространения под управлением Linux или macOS не могут загружать обновления с серверов обновлений "Лаборатории Касперского". Если хотя бы одно устройство с операционной системой Linux или macOS находится в области действия задачи, задача будет иметь статус *Сбой*. Даже если задача успешно завершена на всех устройствах с операционной системой Windows, она вернет ошибку на остальных устройствах.

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и программных модулей для программ "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления программ безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

► *Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для программы Kaspersky Security Center выберите в поле **Тип задачи** выберите **Загрузка обновлений в хранилище точек распространения**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Нажмите на кнопку выбора, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
6. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Запустить**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

9. На закладке **Параметры программы** окна свойств задачи укажите следующие параметры:

- **Источники обновлений**

В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

- Серверы обновлений "Лаборатории Касперского"

  HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

  По умолчанию этот вариант выбран.

- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.

- Локальная или сетевая папка

  Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует аутентификации, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

  > FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

- **Папка для хранения обновлений**

Путь к указанной папке для хранения сохраненных обновлений. Вы можете скопировать указанный путь к папке в буфер обмена. Вы не можете изменить путь к указанной папке для групповой задачи.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий (см. стр. 459).

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

1. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию**

Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

- **Вручную**

  Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию параметр включен.

- **N минут**

  Задача выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени, в день создания задачи.

  По умолчанию задача запускается каждые 30 минут, начиная с текущего системного времени.

- **Каждый N час**

  Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

  По умолчанию задача запускается каждые шесть часов, начиная с текущих системной даты и времени.

- **Каждый N день**

  Задача выполняется регулярно, с заданным интервалом в днях. Также вы можете указать дату и время первого запуска задачи. Эти дополнительные параметры становятся доступны, если они поддерживаются программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

По умолчанию задача запускается каждый понедельник в текущее системное время.

- **Ежедневно (не поддерживает переход на летнее время)**

  Задача выполняется регулярно, с заданным интервалом в днях. Это расписание не поддерживает соблюдение летнего времени. Это значит, что когда время переводят на один час вперед или назад в начале или конце летнего времени, фактическое время запуска задачи не изменяется.

  Не рекомендуется использовать это расписание. Это необходимо для обратной совместимости Kaspersky Security Center.

  По умолчанию задача запускается каждый день в текущее системное время.

- **Еженедельно**

  Задача запускается каждую неделю в указанный день и в указанное время.

- **По дням недели**

  Задача выполняется регулярно, в указанные дни недели, в указанное время.

  По умолчанию задача запускается каждую пятницу в 18:00:00.

- **Ежемесячно**

  Задача выполняется регулярно, в указанный день месяца, в указанное время.

  В месяцах, у которых нет указанного дня, задача выполняется в последний день.

  По умолчанию задача выполняется в первый день каждого месяца, в текущее системное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Задача выполняется регулярно, в указанные дни каждого месяца, в указанное время.

  По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Вирусная атака**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы программ, которые будут отслеживать вирусные атаки. Доступны следующие типы

программ:

- антивирусы для рабочих станций и файловых серверов;
- антивирусы защиты периметра;
- антивирусы для почтовых систем.

По умолчанию выбраны все типы программ.

Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

  Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Например, вы можете запустить задачу управления устройствами с помощью параметра **Включить устройство** и после ее завершения выполнить задачу *Поиск вредоносного ПО*.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию, а для режимов **Вручную**, **Один раз** и **Немедленно** – только на видимых в сети клиентских устройствах. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

  По умолчанию параметр включен.

- **Использовать автоматическое определение случайного интервала между запусками задач**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества

клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

1. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Дополнительно к параметрам, которые вы указываете при создании задачи, вы можете изменить другие параметры этой задачи.

В результате выполнения задачи *Загрузка обновлений в хранилища точек распространения* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа. Загруженные обновления будут использоваться только теми точками распространения, которые входят в указанную группу администрирования и для которых нет явно заданной задачи получения обновлений.

### См. также:

Параметры задачи загрузки обновлений в хранилища точек распространения ..... 929

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" ..... 449

## Включение и выключение автоматической установки обновлений и патчей для компонентов Kaspersky Security Center

Обновления и патчи для Сервера администрирования могут быть установлены только после получения явного одобрения администратором.

Автоматическая установка обновлений для компонентов Kaspersky Security Center включена по умолчанию при установке Агента администрирования на устройство. Вы можете выключить ее при установке Агента администрирования или же выключить позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center при локальной установке Агента администрирования на устройство:*

1. Запустите локальную установку Агента администрирования на устройство (см. стр. 205).
2. На шаге **Дополнительные параметры** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов Kaspersky Security Center со статусом "Не определено"**.
3. Следуйте далее указаниям мастера.

На устройстве будет установлен Агент администрирования с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

► *Чтобы выключить автоматическую установку обновлений для компонентов Kaspersky Security Center при установке Агента администрирования на устройство с помощью инсталляционного пакета:*

1. В главном окне программы перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.
2. Нажмите на пакет **Агент администрирования Kaspersky Security Center <номер версии>**.
3. В окне свойств откройте закладку **Параметры**.
4. Выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.

Агент администрирования будет устанавливаться из этого пакета с выключенной автоматической установкой обновлений и патчей для компонентов Kaspersky Security Center. Вы можете включить автоматическую установку позже с помощью политики.

Если при установке Агента администрирования на устройство флажок был установлен (снят), впоследствии вы можете выключить (включить) автоматическую установку с помощью политики Агента администрирования.

► *Чтобы включить или выключить автоматическую установку обновлений и патчей для компонентов Kaspersky Security Center с помощью политики Агента администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на политику Агента администрирования.
3. В окне свойств политики перейдите на закладку **Параметры программы**.
4. В разделе **Управление патчами и обновлениями** установите включите или выключите переключатель **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**, чтобы включить или выключить автоматическую установку обновлений и патчей.
5. Установите замок (🔒) для этого переключателя.

Политика применится к выбранным устройствам, и автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center будет включена (выключена) на этих устройствах.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center .....476

## Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей программы Kaspersky Endpoint Security для Windows на клиентских устройствах.

► *Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для программы Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.

9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
10. В окне свойств задачи обновления на закладке **Параметры программы** укажите локальный или мобильный режим:

    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.
    - **Мобильный режим**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).

11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей программы для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.
12. Включите параметр **Устанавливать одобренные обновления модулей программ**, чтобы загружать и устанавливать обновления модулей программ вместе с базами программ.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей программы и во время выполнения задачи обновления включает обновления модулей программы в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс программы или через Kaspersky Security Center.

    Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля программы**. При наличии обновлений модулей программы Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей программы – после одобрения их установки администратором.

    Если обновление модулей программы предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то программа устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы программа сохраняла загруженные обновления в папку, а затем укажите путь к папке.

14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.
15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** программа отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых программ.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Одобрение и отклонение обновлений программного обеспечения

Установка обновлений исполняемых программных модулей программ «Лаборатории Касперского», не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программ из безопасного состояния.

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В главном окне программы перейдите в раздел **Операции** → **Программы "Лаборатории Касперского"** → **Обновления**.

   Отобразится список доступных обновлений.

   Для обновлений управляемых программ может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. Выберите обновления, которые требуется подтвердить или отклонить.
3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для программ "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.
Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Обновление Сервера администрирования

Вы можете установить обновления Сервера администрирования с помощью мастера обновления Сервера администрирования.

► *Чтобы установить обновления Сервера администрирования:*

1. В главном окне программы перейдите в раздел **Операции** → **Программы "Лаборатории Касперского"** → **Обновления**.
2. Откройте мастер обновления Сервера администрирования одним из следующих способов:
   - Нажмите на обновление в списке обновлений и в открывшемся окне перейдите по ссылке **Запустить мастер обновления Сервера администрирования** .
   - Перейдите по ссылке **Запустить мастер обновления Сервера администрирования** в поле уведомления в верхней части окна программы.
3. Чтобы указать, когда устанавливать обновление, в окне мастера обновления Сервера администрирования выберите один из следующих вариантов:
   - **Установить сейчас**. Выберите этот вариант, если вы хотите установить обновления сейчас.
   - **Отложить установку**. Выберите этот вариант, если вы хотите установить обновления позже. В этом случае будет отображаться уведомление об этом обновлении.
   - **Игнорировать это обновление**. Выберите этот вариант, если вы не хотите устанавливать обновление и не хотите получать уведомления об этом обновлении.
4. Если вы хотите создать резервную копию Сервера администрирования перед установкой обновления, выберите параметр **Сделать резервную копию Сервера администрирования перед установкой обновления**.
5. Нажмите на кнопку **ОК**, чтобы закрыть окно мастера.

В процессе резервного копирования прерывается процесс установки обновлений.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Включение и выключение офлайн-модели получения обновлений

Не рекомендуется выключать офлайн-модель получения обновлений. Выключение может привести к сбоям в доставке обновлений на устройства. В некоторых случаях специалисты Службы технической поддержки "Лаборатории Касперского" могут рекомендовать вам выключить параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее**. Тогда вам нужно будет убедиться, что задача загрузки обновлений в хранилище для программ "Лаборатории Касперского" настроена.

► *Чтобы включить или выключить офлайн-модель получения обновлений для группы администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Нажмите на кнопку **Группы**.
3. В списке групп администрирования выберите группу администрирования, для которой требуется включить офлайн-модель получения обновлений.
4. Нажмите на политику Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

   По умолчанию параметры дочерней политики наследуют параметры родительской политики и не могут быть изменены. Если политика, которую вы хотите изменить, унаследована, то вам нужно создать политику для Агента администрирования в требуемой группе администрирования. В созданной политике вы можете изменить параметры, которые не заблокированы в родительской политике.
5. На закладке **Параметры программы** выберите раздел **Управление патчами и обновлениями**.
6. Включите или выключите параметр **Загружать обновления и антивирусные базы с Сервера администрирования заранее (рекомендуется)**, чтобы включить или выключить офлайн-модель получения обновлений соответственно.

   По умолчанию офлайн-модель получения обновлений включена.

В результате офлайн-модель получения обновлений будет включена или выключена.

kaspersky

См. также:



# Обновление баз и программных модулей "Лаборатории Касперского" на автономных устройствах

Обновление баз и программных модулей "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление (см. стр. 449) с помощью хранилища Сервера администрирования или хранилищ точек распространения.

Когда вам необходимо обновить базы данных и программные модули на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

  Чтобы хранилище Сервера администрирования содержало обновления, необходимые для программы безопасности, установленной на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должна быть установлена эта программа безопасности. Эта программа должна быть настроена на получение обновлений из хранилища Сервера администрирования с помощью задачи Загрузка обновлений в хранилище Сервера администрирования.

- Любого устройства, на котором установлена такая же программа безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и программных модулей путем копирования их из хранилища Сервера администрирования.

► *Чтобы обновить базы данных и программные модули "Лаборатории Касперского" на автономных устройствах:*

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.
2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены: \\<server name>\KLSHARE\Updates.

   Также вы можете настроить в Kaspersky Security Center регулярное копирование обновлений в выбранную вами папку. Для этого используйте параметр **Копировать полученные обновления в дополнительные папки** в свойствах задачи загрузки обновлений в хранилище Сервера администрирования. Если вы укажете папку, расположенную на запоминающем устройстве или внешнем жестком диске, в качестве папки назначения для этого параметра, это запоминающее устройство всегда будет содержать последнюю версию обновлений.

3. На автономных устройствах настройте программу безопасности (например, настройте Kaspersky Endpoint Security для Windows) на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.
4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.
5. На автономном устройстве, на которое требуется установить обновления, запустите задачу обновления Kaspersky Endpoint Security для Windows.

После завершения задачи обновления базы данных и программные модули "Лаборатории Касперского" будут обновлены на устройстве.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

Создание задачи Загрузка обновлений в хранилище Сервера администрирования .....1244

## Резервное копирование и восстановление веб-плагинов

Kaspersky Security Center 14.2 Web Console позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Например, вы можете создать резервную копию данных веб-плагина перед его обновлением до более новой версии. После обновления, если более новая версия не соответствует вашим требованиям или ожиданиям, вы можете восстановить предыдущую версию веб-плагина из резервной копии данных.

► *Для резервного копирования данных веб-плагинов:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Веб-плагины**.

   Откроется окно **Параметры консоли**.
2. На закладке **Веб-плагины** выберите веб-плагины, для которых требуется создать резервную копию данных и нажмите на кнопку **Создать резервную копию данных**.

Резервное копирование данных выбранных веб-плагинов. Вы можете просмотреть созданные резервные копии данных на закладке **Резервные копии данных**.

► *Чтобы восстановить веб-плагин из резервной копии данных:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Резервные копии**.

   Откроется окно **Параметры консоли**.
2. На закладке **Резервные копии данных** выберите резервную копию данных веб-плагина, который вы хотите восстановить, а затем нажмите на кнопку **Восстановить из резервной копии данных**.

Веб-плагин восстанавливается из выбранной резервной копии данных.

## Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*. В этом случае область действия политик задается с помощью тегов, местоположения устройств в подразделениях Active Directory, членства в группах безопасности Active Directory (см. стр. 426).

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;
- множество небольших изолированных офисов;

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

## См. также:



## В этом разделе



## Типовая конфигурация точек распространения: один офис

В типовой конфигурации "один офис" все устройства находятся в сети организации и "видят" друг друга. Сеть организации может состоять из нескольких выделенных частей (сетей или сегментов сети), связанных узкими каналами.

Возможны следующие способы построения структуры групп администрирования:

- Построение структуры групп администрирования с учетом топологии сети. Структура групп администрирования не обязательно должна точно отражать топологию сети. Достаточно того, чтобы

выделенным частям сети соответствовали какие-либо группы администрирования. Можно использовать автоматическое назначение точек распространения, либо назначать точки распространения вручную.

- Построение структуры групп администрирования, не отражающей топологию сети. В этом случае следует отключить автоматическое назначение точек распространения и в каждой выделенной части сети назначить одно или несколько устройств точками распространения на корневую группу администрирования, например, на группу **Управляемые устройства**. Все точки распространения окажутся на одном уровне и будут иметь одинаковую область действия "все устройства сети организации". Каждый Агент администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert.

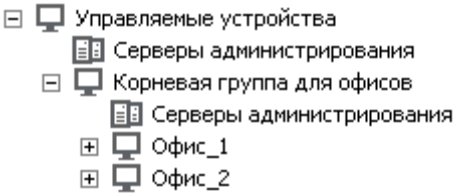
## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Типовая конфигурация точек распространения: Множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).




На каждую группу администрирования, соответствующую офису, нужно назначить одну или несколько точек распространения. Точками распространения нужно назначать устройства удаленного офиса, имеющие достаточно места на диске. Устройства, размещенные, например, в группе **Офис 1**, будут обращаться к точкам распространения, назначенным на группу администрирования **Офис 1**.

Если некоторые пользователи физически перемещаются между офисами с ноутбуками, нужно в каждом удаленном офисе дополнительно к упомянутым выше точкам распространения выбрать два и или более устройств и назначить их точками распространения на группу администрирования верхнего уровня (группа **Корневая группа для офисов** на рисунке выше).

Пример: Ноутбук находится в группе администрирования **Офис 1**, но физически переехавший в офис, соответствующий группе **Офис 2**. После перемещения Агент администрирования на ноутбуке попытается обратиться к точкам распространения, назначенным на группу **Офис 1**, но эти точки распространения окажутся недоступны. Тогда Агент администрирования начнет обращаться к точкам распространения, назначенным на группу **Корневая группа для офисов**. Так как удаленные офисы изолированы друг от друга, то из всех точек распространения, назначенных на группу администрирования **Корневая группа для офисов**, успешными будут лишь обращения к точкам распространения, назначенным на группу **Офис 2**. То есть ноутбук, оставаясь в группе администрирования, соответствующей своему исходному офису, будет, тем не менее, использовать точку распространения того офиса, в котором в данный момент находится физически.

## О назначении точек распространения

Вы можете назначить управляемое устройство в качестве точки распространения вручную (см. стр. 1266) или автоматически (см. стр. 1266).

Если вы назначаете управляемое устройство в качестве точки распространения вручную, вы можете выбрать любое устройство в своей сети.

Если вы назначаете точки распространения автоматически, Kaspersky Security Center может выбрать только то управляемые устройства, которые соответствует следующим условиям:

- Устройство должно иметь не менее 50 ГБ свободного места на диске.
- Управляемое устройство подключается к Kaspersky Security Center напрямую (не через шлюз).
- Управляемое устройство не является ноутбуком.

> Если в вашей сети нет устройств, соответствующих заданным условиям, Kaspersky Security Center не будет автоматически назначать какое-либо устройство точкой распространения.

## Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать (см. стр. 1266), какие устройства назначать точками распространения.

► *Чтобы назначить точки распространения автоматически:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Точки распространения**.
3. Выберите параметр **Автоматически назначать точки распространения**.

   > Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.
4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Назначение точек распространения вручную

Kaspersky Security Center позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, какие устройства назначать точками распространения. Однако если вы по какой-то причине хотите отказаться от автоматического назначения точек распространения (например, если вы хотите использовать специально выделенные серверы), вы можете назначать точки распространения вручную, предварительно рассчитав их количество и конфигурацию (см. стр. 167).

Устройства, выполняющие роль точек распространения, должны быть защищены, в том числе физически, от любого типа несанкционированного доступа.

► *Чтобы вручную назначить устройство точкой распространения:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Точки распространения**.
3. Выберите параметр **Вручную назначать точки распространения**.
4. Нажмите на кнопку **Назначить**.
5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.
6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.
7. Нажмите на кнопку **ОК**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.
8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.
9. В окне свойств настройте параметры точки распространения:
   - В разделе **Общие** укажите параметр взаимодействия точки распространения с клиентскими устройствами.
     - **SSL-порт**

       Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

       По умолчанию номер порта – 13000.
     - **Использовать многоадресную IP-рассылку**

       Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

       Многоадресная IP-рассылка уменьшает время, необходимое для установки программ из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке программы на одно клиентское устройство.
     - **Адрес IP-рассылки**

       IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

По умолчанию Kaspersky Security Center автоматически назначает уникальный IP-адрес многоадресной рассылки в заданном диапазоне.

- **Номер порта IP-рассылки**

  Номер порта многоадресной рассылки.

  Номер порта по умолчанию – 15001. Если в качестве точки распространения указано устройство, на котором установлен Сервер администрирования, то для подключения с использованием SSL-протокола по умолчанию используется порт 13001.

- **Адрес точки распространения для удаленных устройств**
- Распространять обновления

  Обновления распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения обновлений, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить (см. стр. 167) количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок обновлений и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Распространять инсталляционные пакеты**

  Инсталляционные пакеты распространяются на управляемые устройства из следующих источников:

  - Эта точка распространения, если этот параметр включен.
  - Другие точки распространения, Сервер администрирования или серверы обновлений "Лаборатории Касперского", если параметр выключен.

  Если вы используете точки распространения для распространения инсталляционных пакетов, вы можете сэкономить трафик, так как уменьшите количество загрузок. Также вы можете снизить нагрузку на Сервер администрирования и перераспределить нагрузку между точками распространения. Вы можете вычислить (см. стр. 167) количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

  Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Запустить push-сервер**
- Порт push-сервера

- В разделе **Область действия** укажите область, на которую точка распространения распространяет обновления (группы администрирования и / или сетевое местоположение).

> Только устройства под управлением операционной системы Windows могут определять свое сетевое местоположение. Определение сетевого местоположения недоступно для устройств под управлением других операционных систем.

- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Источник обновлений** можно выбрать источник обновлений для точки распространения:
  - **Источник обновлений**
  - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. стр. 459) .

По умолчанию параметр включен.

- В разделе **Параметры подключения к интернету** можно настроить параметры доступа в интернет:
  - **Использовать прокси-сервер**

    Если флажок установлен, в полях ввода можно настроить параметры подключения к прокси-серверу.

    По умолчанию флажок снят.
  - **Адрес прокси-сервера**

    Адрес прокси-сервера.
  - **Номер порта**

    Номер порта, по которому будет выполняться подключение.
  - **Не использовать прокси-сервер для локальных адресов**

    Если параметр включен, то при подключении к устройствам в локальной сети не используется прокси-сервер.

    По умолчанию параметр выключен.
  - **Аутентификация на прокси-сервере**

    Если флажок установлен, в полях ввода можно указать учетные данные для аутентификации на прокси-сервере.

    По умолчанию флажок снят.
  - **Имя пользователя**

    Учетная запись пользователя, от имени которой будет выполняться подключение к прокси-серверу.
  - **Пароль**

    Пароль учетной записи, от имени которой будет запускаться задача.
- В разделе **Прокси-сервер KSN** вы можете настроить программу так, чтобы точка распространения использовалась для пересылки KSN запросов от управляемых устройств.
  - **Включить прокси-сервер KSN на стороне точки распространения**

    Служба прокси-сервера KSN выполняется на устройстве, которое выполняет роль точки распространения. Используйте этот параметр для перераспределения и

оптимизации трафика сети.

Точка распространения отправляет статистику KSN, указанную в Положении о Kaspersky Security Network, в "Лабораторию Касперского". По умолчанию Положение о KSN расположено в папке %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

По умолчанию параметр выключен. Включение этого параметра вступает в силу только в том случае, если параметры **Использовать Сервер администрирования как прокси-сервер** и **Я принимаю условия использования Kaspersky Security Network** включены(см. стр. 830) в окне свойств Сервера администрирования.

Можно назначить узлу отказоустойчивого кластера с холодным резервом (активный / пассивный) точку распространения и включить прокси-сервер KSN на этом узле.

- **Пересылать KSN запрос Серверу администрирования**

  Точка распространения пересылает KSN запросы от управляемых устройств Серверу администрирования.

  По умолчанию параметр включен.

- **Доступ к облачной службе KSN/Локальному KSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или Локальному KSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или Локальный KSN.

  Точки распространения с установленным Агентом администрирования версии 11 (или более ранней) не могут напрямую обращаться к Локальному KSN. Если вы хотите перенастроить точки распространения для отправки запросов KSN в Локальный KSN, включите параметр **Пересылать KSN запросы Серверу администрирования** для каждой точки распространения.

  Точки распространения с установленным Агентом администрирования версии 12 (и выше) могут напрямую обращаться к Локальному KSN.

- **Игнорировать параметры прокси-сервера для подключения к Локальному KSN**

  Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали Локальный KSN напрямую. В противном случае запрос от управляемой программы не будет передан в Локальный KSN.

  Это параметр доступен, если вы выбрали параметр **Доступ к облачной-службе KSN/Локальному KSN непосредственно через интернет**.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **Использовать UDP-порт**

- **UDP-порт**

- Если точка распространения работает на машине, отличной от Сервера администрирования, в разделе **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:

  - **Шлюз соединения**

- **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**
- **Открыть локальный порт для Kaspersky Security Center Web Console**
- **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**
- **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

- Настройте опрос доменов Windows, Active Directory и IP-диапазонов точкой распространения:
  - **Windows-домены**

    Вы можете включить обнаружение устройств для Windows-доменов и задать его расписание.
  - **Active Directory**

    Вы можете включить опрос Active Directory и задать расписание опроса.

    Если вы установили флажок **Разрешить опрос Active Directory**, выберите один из следующих вариантов:

    - **Опросить текущий домен Active Directory**.
    - **Опросить лес доменов Active Directory**.
    - **Опросить указанные домены Active Directory**. Если вы выбрали этот вариант, добавьте один или несколько доменов Active Directory в список.
  - IP-диапазоны

    Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

    Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов (см. стр. 667).

    Если включить параметр **Включить опрос с помощью технологии Zeroconf**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вы должны установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных:
  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.
  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **ОК**.

В результате выбранные устройства будут выполнять роль точек распространения.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

► *Чтобы просмотреть и изменить список точек распространения для группы администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
3. В открывшейся панели слева выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения.

   Для этого используйте пункт меню **Точки распространения**.
4. В главном окне программы перейдите в раздел **Устройства** → **Точки распространения**.
5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить** над списком управляемых устройств и выберите устройства в открывшейся панели.
6. Чтобы удалить назначенные точки распространения, выберите устройства из списка и нажмите на кнопку **Отменить назначение**.

В зависимости от изменений, точки распространения добавляются в список или существующие точки распространения удаляются из списка.

### См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

## Принудительная синхронизация

Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, но в некоторых случаях вам может потребоваться запустить синхронизацию для указанного устройства принудительно. Вы можете запустить принудительную синхронизацию для следующих устройств:

- Устройств с установленным Агентом администрирования.
- Устройств под управлением KasperskyOS.

  Перед запуском принудительной синхронизации для устройства под управлением KasperskyOS убедитесь, что устройство включено в область действия точки распространения и что на точке распространения включен push-сервер (см. стр. 1274).
- iOS-устройств.
- Android-устройств.

Перед запуском принудительной синхронизации для Android-устройства необходимо настроить Google Firebase Cloud Messaging.

**Синхронизация одного устройства**

► *Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать принудительно**.

Программа выполняет синхронизацию выбранного устройства с Сервером администрирования.

**Синхронизация нескольких устройств**

► *Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:*

1. Откройте список устройств группы администрирования или выборку устройств:
   - В главном меню перейдите в раздел **Устройства** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** над списком управляемых устройств и выберите группу администрирования, в которую входят устройства для синхронизации
   - Запустите выборку устройств (см. стр. 1146), чтобы просмотреть список устройств.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием ( ••• ) и нажмите на кнопку **Синхронизировать принудительно**.

   Программа выполняет синхронизацию выбранных устройств с Сервером администрирования.
4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав кнопку на **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

**Просмотр времени доставки политики**

После изменения политики для программы "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

► *Чтобы просмотреть дату и время доставки политики программы на управляемые устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Перейдите на закладку **Программы**.

4. Выберите программу, для которой требуется посмотреть дату синхронизации политики.

   Откроется окно политики программы, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

## См. также:


Настройка и распространение политик: подход, ориентированный на устройства ..... 402

Сценарий: Настройка защиты сети ..... 400

Включение push-сервера ..... 1274


## Включение push-сервера

В Kaspersky Security Center точка распространения может работать как push-сервер для устройств, которые управляются по мобильному протоколу и для устройств под управлением Агента администрирования. Например, push-сервер должен быть включен, если вы хотите включить принудительную синхронизацию (см. стр. 1272) устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемой программы или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

► *Чтобы включить push-сервер на точке распространения:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Точки распространения**.
3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.
4. В разделе **Общие** включите параметр **Запустить push-сервер**.
5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.
6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.
7. Нажмите на кнопку **ОК**.

Push-сервер включен на выбранном устройстве.

kaspersky

### См. также:



# Управление программами сторонних производителей на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center связанные с управлением сторонних программами на клиентских устройствах.

### В этом разделе



## О программах сторонних производителей

Kaspersky Security Center может помочь вам обновить программы сторонних производителей, установленное на клиентских устройствах, и исправить уязвимости программ сторонних производителей. Kaspersky Security Center может обновлять программы сторонних производителей только с текущей версии до последней версии. В следующем списке представлены программы сторонних производителей, которые вы можете обновить с помощью Kaspersky Security Center:

Список программ сторонних производителей может обновляться и увеличиваться за счет новых программ. Вы можете проверить, можете ли вы обновить программу сторонних производителей (установленную на устройствах пользователей) с помощью Kaspersky Security Center, просмотрев список доступных обновлений в Kaspersky Security Center 14.2 Web Console (см. стр. 1285).

- 7-Zip Developers: 7-Zip.
- Adobe Systems:
  - Adobe Acrobat DC;

  - Adobe Acrobat Reader DC;
  - Adobe Acrobat;
  - Adobe Reader;
  - Adobe Shockwave Player.
- AIMPDevTeam: AIMP.
- ALTAP: Altap Salamander.
- Apache Software Foundation: Apache Tomcat.
- Apple:
  - Apple iTunes;
  - Apple QuickTime.
- Armory Technologies, Inc.: Armory.
- Cerulean Studios: Trillian Basic.
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber.
- Code Sector: TeraCopy.
- Codec Guide:
  - K-Lite Codec Pack Basic;
  - K-Lite Codec Pack Full;
  - K-Lite Codec Pack Mega;
  - K-Lite Codec Pack Standard.
- DbVis Software AB: DbVisualizer.
- Decho Corp.:
  - Mozy Enterprise;
  - Mozy Home;
  - Mozy Pro.
- Dominik Reichl: KeePass Password Safe.
- Don HO don.h@free.fr: Notepad++.
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox.
- EaseUs: EaseUS Todo Backup Free.
- Electrum Technologies GmbH: Electrum.
- Enter Srl: Iperius Backup.
- Eric Lawrence: Fiddler.
- EverNote: EverNote,
- Exodus Movement Inc: Exodus.

- EZB Systems: UltraISO.
- Famatech:
  - Radmin.
  - Remote Administrator.
- Far Manager: FAR Manager.
- FastStone Soft: FastStone Image Viewer.
- FileZilla Project: FileZilla.
- Firebird Developers: Firebird.
- Foxit Corporation:
  - Foxit Reader;
  - Foxit Reader Enterprise.
- Free Download Manager.ORG: Free Download Manager.
- GIMP project: GIMP.
- GlavSoft LLC.: TightVNC.
- GNU Project: Gpg4win
- Google:
  - Google Earth;
  - Google Chrome;
  - Google Chrome Enterprise;
  - Google Earth Pro;
- Inkscape Project: Inkscape.
- IrfanView: IrfanView.
- iterate GmbH: Cyberduck.
- Logitech: SetPoint.
- LogMeIn, Inc.:
  - LogMeIn;
  - Hamachi;
  - LogMeIn Rescue Technician Console.
- Martin Prikryl: WinSCP.
- Mozilla Foundation:
  - Mozilla Firefox;
  - Mozilla Firefox ESR;
  - Mozilla SeaMonkey;
  - Mozilla Thunderbird.
- New Cloud Technologies Ltd: MyOffice Standard. Home Edition.

- OpenOffice.org: OpenOffice.
- Open Whisper Systems: Signal
- Opera Software: Opera.
- Oracle Corporation:
  - Oracle Java JRE;
  - Oracle VirtualBox.
- PDF44: PDF24 MSI/EXE.
- Piriform:
  - CCleaner;
  - Defraggler;
  - Recuva;
  - Speccy.
- Postgresql: PostgreSQL.
- RealNetworks: RealPlayer Cloud.
- RealVNC:
  - RealVNC Server;
  - RealVNC Viewer.
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum).
- Simon Tatham: PuTTY.
- Skype Technologies: Skype for Windows.
- Sober Lemur S.a.s.:
  - PDFsam Basic;
  - PDFsam Visual.
- Softland: FBackup.
- Splashtop Inc.: Splashtop Streamer.
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP.
- Sublime HQ Pty Ltd: Sublime Text.
- TeamViewer GmbH:
  - TeamViewer Host;
  - TeamViewer.
- Telegram Messenger LLP: Telegram Desktop.
- The Document Foundation:
  - LibreOffice;
  - LibreOffice HelpPack.
- The Git Development Community:

    - Git for Windows;
    - Git LFS.
- The Pidgin developer community: Pidgin.
- TortoiseSVN Developers: TortoiseSVN.
- VideoLAN: VLC media player.
- VMware:
    - VMware Player;
    - VMware Workstation.
- WinRAR Developers: WinRAR.
- WinZip: WinZip.
- Wireshark Foundation: Wireshark.
- Wrike: Wrike.
- Zimbra: Zimbra Desktop.

### См. также:

Сценарий:Обновление программ сторонних производителей ..... 489
Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516
Об обновлениях программ сторонних производителей ..... 1284

## Установка обновлений программ сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center, относящиеся к установке обновлений для программ сторонних производителей, установленных на клиентских устройствах.

kaspersky

## В этом разделе



## Сценарий: Обновление программ сторонних производителей

В этом разделе представлен сценарий обновления программ сторонних производителей, установленных на клиентских устройствах. Программы сторонних производителей включают в себя программы от Microsoft и других поставщиков программного обеспечения (см. стр. 1275). Обновления для программ Microsoft предоставляются службой Центра обновления Windows.

### Предварительные требования

Сервер администрирования должен иметь подключение к интернету для установки обновлений программ сторонних производителей, отличных от программ Microsoft.

По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений программ Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления программ Microsoft непосредственно с серверов обновлений Microsoft или с Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации. Если вы используете Сервер администрирования в качестве сервера WSUS, Сервер администрирования должен быть подключен к интернету.

### Этапы

Обновление производителей состоит из следующих этапов:

a. **Поиск требуемых обновлений**

Чтобы найти обновления программ сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу или запустите мастер первоначальной настройки.

Инструкции:

- Консоль администрирования: Поиск уязвимостей в программах (см. стр. 522), Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (см. стр. 1289), параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

**b. Анализ списка найденных обновлений**

Просмотрите список **Обновление программного обеспечения** и решите, какие обновления следует установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации о доступных обновлениях (см. стр. 492).
- Kaspersky Security Center 14.2 Web Console: Просмотр информации о доступных обновлениях программ сторонних производителей (см. стр. 1305).

**c. Настройка установки обновлений**

После того как Kaspersky Security Center получает список обновлений программ сторонних производителей, вы можете установить их на клиентские устройства, используя задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Создайте одну из этих задач. Вы можете создать эти задачи на закладке **Задачи** или с помощью списка **Обновление программного обеспечения**.

Задача *Установка требуемых обновлений и закрытия уязвимостей* используется для установки обновлений для программ Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления программ других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

Для установки некоторых обновлений программного обеспечения вы должны принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Инструкции:

- Консоль администрирования: Закрытие уязвимостей в программах (см. стр. 527), Просмотр информации о доступных обновлениях (см. стр. 492).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295), Создание задачи Установка обновлений Центра обновления Windows (см. стр. 1303), Просмотр информации о доступных обновлениях программ сторонних производителей (см. стр. 1305).

**d. Задание расписания задачи**

Чтобы убедится, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При планировании задачи *Установка обновлений Центра обновления Windows* обратите внимание, что для этой задачи вы должны определять список обновлений каждый раз перед запуском этой задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

**e. Одобрение и отклонение обновлений программного обеспечения (если требуется)**

Если вы создали задачу Установка требуемых обновлений и закрытие уязвимостей, вы можете указать правила установки обновлений в свойствах задачи. Если вы создали задачу Установка обновлений Центра обновления Windows, пропустите этот шаг.

Для каждого правила вы можете определить обновления для установки в зависимости от статуса обновления: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только обновлений Центра обновления Windows и только тех, которые имеют статус *Одобрено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления Центра обновления Windows со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения** (**Операции** → **Управление патчами** → **Обновления программного обеспечения**).

Инструкции:

- Консоль администрирования: Одобрение и отклонение обновлений программного обеспечения (см. стр. 493).
- Kaspersky Security Center 14.2 Web Console: Одобрение и отклонение обновлений программ сторонних производителей (см. стр. 1308).

**f. Настройка Сервера администрирования для работы в качестве службы Windows Server Update Services (WSUS) (если требуется)**

По умолчанию обновления Центра обновления Windows загружаются на управляемые устройства с серверов Microsoft. Вы можете изменить этот параметр, чтобы использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования синхронизирует данные обновления с Центром обновления Windows с заданной периодичностью и предоставляет обновления централизовано службам Центра обновления Windows на сетевых устройствах.

Чтобы использовать Сервер администрирования в качестве сервера WSUS, создайте задачу Синхронизация обновлений Windows Update и установите флажок **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования.

Инструкции:

- Консоль администрирования: Синхронизация обновлений Windows Update с Сервером администрирования (см. стр. 494), Настройка обновлений Windows в политике Агента администрирования (см. стр. 513).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Синхронизация обновлений Windows Update (см. стр. 1309).

**g. Запуск задачи установки обновлений**

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. После запуска этих задач, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

**h. Создание отчета о результатах установки обновлений программ сторонних производителей (если требуется)**

Для просмотра статистики установки обновлений создайте **Отчет о результатах установки обновлений стороннего ПО**.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (см. стр. 588)
- Kaspersky Security Center 14.2 Web Console: Генерация и просмотр отчета (см. стр. 1372)

**Результаты**

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

Если вы создали задачу *Установка обновлений Центра обновления Windows*, будут установлены только те обновления, которые указаны в свойствах задачи *Установка обновлений Центра обновления Windows*. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу *Установка обновлений Центра обновления Windows*.

kaspersky

## См. также



## Об обновлениях программ сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями программного обеспечения сторонних производителей, установленных на управляемых устройствах, и закрывать уязвимости в программах Microsoft и других производителей программного обеспечения с помощью установки необходимых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на устройства.

Обновление некоторых программ Kaspersky Security Center выполняет путем удаления предыдущей версии программы и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений программ сторонних производителей, которые можно установить с помощью Системного администрирования. Кроме того, специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных)

или недокументированных возможностей в таких обновлениях, и не проводят другие виды анализа упомянутых выше обновлений.

**Задачи для установки обновлений программ сторонних производителей**

Когда метаданные обновлений программ сторонних производителей загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив следующие задачи:

- Задача *Установка требуемых обновлений и закрытия уязвимостей* (см. стр. 1295).

  Задача *Установка требуемых обновлений и закрытия уязвимостей* используется для установки обновлений для программ Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления программ других поставщиков. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование.

  После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

- Задача *Установка обновлений Центра обновления Windows* (см. стр. 1303).

  Задача *Установка обновлений Центра обновления Windows* не требует лицензии, но ее можно использовать только для установки обновлений Центра обновления Windows.

  После завершения работы этой задачи устанавливаются только те обновления, которые указаны в свойствах задачи. Позже, если вы захотите установить новые обновления, загруженные в хранилище Сервера администрирования, вам будет необходимо добавить требуемые обновления в список обновлений существующей задачи или создать задачу Установка обновлений Центра обновления Windows.

**Использовать Сервер администрирования в роли WSUS-сервера**

Информация о доступных обновлениях Microsoft Windows передается из центра обновлений Windows. Сервер администрирования может использоваться в роли сервера Windows Update (WSUS). Чтобы использовать Сервер администрирования в качестве WSUS-сервера, вы должны создать задачу Синхронизация обновлений Windows Update и включить параметр **Использовать Сервер администрирования в роли WSUS-сервера** в политике Агента администрирования (см. стр. 750). После настройки синхронизации данных с центром обновлений Windows Сервер администрирования с заданной периодичностью централизованно предоставляет обновления службам Windows Update на устройствах.

## Установка обновлений программ сторонних производителей

Вы можете установить обновления программ сторонних производителей на управляемые устройства, создав и запустив одну из следующих задач:

- *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295)

  Вы можете создать задачу *Установка требуемых обновлений и закрытия уязвимостей*, только если у вас есть лицензия на Системное администрирование. Эту задачу можно использовать для установки обновлений Центра обновления Windows, предоставленных Microsoft, и обновлений программ других поставщиков.

- *Установка обновлений Центра обновления Windows* (см. стр. 1303)

  Задача *Установка обновлений Центра обновления Windows* используется только для установки обновлений Центра обновления Windows.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

  В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

  Мастер установки обновления доступен при наличии лицензии на Системное администрирование (см. стр. 353).

  Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

**Установка обновлений программ сторонних производителей с помощью списка обновлений**

► *Чтобы установить обновления программ сторонних производителей:*

1. Откройте один из списков обновлений:
   - Чтобы открыть список общих обновлений, перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.
   - Чтобы открыть список обновлений для управляемого устройства, перейдите в раздел **Устройства** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Применимые обновления**.
   - Чтобы открыть список обновлений для определенной программы, перейдите в раздел **Операции** → **Программы сторонних производителей** → **Реестр программ** → <название программы> → **Применимые обновления**.

   Отобразится список доступных обновлений.
2. Установите флажки рядом с теми обновлениями, которые вы хотите установить.
3. Нажмите на кнопку **Установить обновления**.

   Для установки некоторых обновлений программного обеспечения вы должны принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не установятся.
4. Выберите один из следующих вариантов:
   - **Новая задача.**

     Запустится мастер создания задачи (см. стр. 1111). Если у вас есть лицензия на Системное администрирование (см. стр. 353), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Установка обновлений Центра обновления Windows*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

- **Установить обновление (добавить правило в указанную задачу).**

  Выберите задачу, в которую вы хотите добавить выбранные обновления. Если у вас есть лицензия на Системное администрирование (см. стр. 353), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Новое правило для установки выбранных обновлений будет автоматически добавлено в выбранную задачу. Если у вас нет лицензии, по умолчанию выбран тип задачи *Установка обновлений Центра обновления Windows*. Выбранные обновления добавлены в свойства задачи.

  Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Устройства → Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Чтобы установить обновления программ сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или задачу *Установка обновлений Центра обновления Windows*. Вы можете запустить эти задачи вручную (см. стр. 1112) или задать расписание в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

**Установка обновлений программ сторонних производителей с помощью мастера установки обновлений**

Мастер установки обновления доступен при наличии лицензии на Системное администрирование (см. стр. 353).

► *Чтобы создать задачу установки обновлений программ сторонних производителей с помощью мастера установки обновления:*

1. В главном окне программы перейдите в раздел **Операции → Управление патчами → Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

2. Установите флажок рядом с обновлением, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытия уязвимостей.*
   - *Установка обновлений Центра обновления Windows.*
   - *Закрытие уязвимостей.*

   Вы не можете изменить задачи двух последних типов для установки новых обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливают выбранное вами обновление, включите параметр **Показать только задачи, которые устанавливают обновление**.
5. Выберите действие, которое хотите выполнить:

- Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.
- Чтобы добавить новое правило в существующую задачу:
  a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.
  b. На открывшейся странице настройте новое правило:
     - **Правило установки обновлений данного уровня важности**
     - **Правило установки обновлений данного уровня важности по MSRC**
     - **Правило установки обновлений данного поставщика**
     - **Правило установки обновлений типа**
     - **Правило установки выбранного обновления**
     - **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

a. Нажмите на кнопку **Добавить**.

- Чтобы создать задачу:
  a. Нажмите на кнопку **Новая задача**.
  b. На открывшейся странице настройте новое правило:
     - **Правило установки обновлений данного уровня важности**
     - **Правило установки обновлений данного уровня важности по MSRC**
     - **Правило установки обновлений данного поставщика**
     - **Правило установки обновлений типа**
     - **Правило установки выбранного обновления**
     - **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

a. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью (см. стр. 1295) мастера создания задачи. Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

## См. также:

Сценарий:Обновление программ сторонних производителей .....489

## Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи Поиск уязвимостей и требуемых обновлений Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, установленных на управляемых устройствах.

Задача Поиск уязвимостей и требуемых обновлений создается автоматически во время работы мастера первоначальной настройки (см. стр. 1007). Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

► *Чтобы создать задачу Поиск уязвимостей и требуемых обновлений:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для программы Kaspersky Security Center выберите тип задачи **Поиск уязвимостей и требуемых обновлений**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112).
10. На закладке **Параметры программы** настройте следующие параметры:

    - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних программ.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

  Агент Центра обновления Windows на клиентском устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. 750)).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в программах**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение

задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления только если параметр **Соединяться с сервером обновлений для актуализации данных** включен и параметр **Активный** включен в группе параметров **Режим поиска обновлений Windows Update**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска обновлений Windows Update** или если параметр **Соединяться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Активный**.
- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Выключен**, Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке

%WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

## См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

Сценарий:Обновление программ сторонних производителей .....489

## Параметры задачи поиска уязвимостей и требуемых обновлений

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

Помимо общих параметров задачи (см. стр. 1112), вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних программ.

По умолчанию параметр включен.

- **Соединяться с сервером обновлений для актуализации данных**

Агент Центра обновления Windows на клиентском устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

- Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования (см. стр. 750)).
- Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
- Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в программах**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления только если параметр **Соединяться с сервером обновлений для актуализации данных** включен и параметр **Активный** включен в группе параметров **Режим поиска обновлений Windows Update**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска обновлений Windows Update** или если параметр **Соединяться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Активный**.
- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Режим поиска обновлений Windows Update** выбран параметр **Выключен**, Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите способ**

**дополнительного поиска программ в файловой системе**. Полный список поддерживаемых программ сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для программ сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних программ.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска программ в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних программ, требующих устранения уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены программы. По умолчанию список содержит системные папки, в которые устанавливается большинство программ.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

**Рекомендации по настройке расписания запуска задачи**

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на

процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

См. также:



## Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование(см. стр. 353).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в программах сторонних производителей, включая программы Microsoft, установленные на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений (см. стр. 1285) или мастер закрытия уязвимостей (см. стр. 1316).
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновлений (см. стр. 1299) в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

► *Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для программы Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. стр. 1192) **Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите правила для установки обновления (см. стр. 1299), а затем следующие параметры:
   - **Начинать установку в момент перезагрузки или выключения устройства**

Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

По умолчанию параметр выключен.

- **Устанавливать необходимые общесистемные компоненты**

  Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

  Если этот параметр выключен, необходимо установить пререквизиты вручную.

  По умолчанию параметр выключен.

- **Разрешать установку новой версии программы при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

  Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать

трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, программа с определенной частотой предлагает

пользователю выполнить перезагрузку операционной системы.

По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием программы в заблокированных сессиях через (мин)**

  Принудительное завершение работы программ, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа программ на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа программ на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

2. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
3. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
4. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
5. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.
6. Нажмите на кнопку **Сохранить**.

   Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

## См. также:


Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

Об обновлениях программ сторонних производителей ..... 1284

kaspersky

## Добавление правил для установки обновлений

Эта функциональность доступна при наличии лицензии на Системное администрирование (см. стр. 353).

При установке обновлений программного обеспечения или закрытии уязвимостей в программах с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений программ сторонних производителей (то есть программ производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления программ сторонних производителей вы можете выбрать программы и версии программ, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295).
- Добавить правило на закладке **Параметры программы** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений (см. стр. 1285) или мастера закрытия уязвимостей (см. стр. 1316).

► Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. В окне **Тип правила** выберите **Правило для всех обновлений**.
3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:
   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.
   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те

обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Обновления** выберите обновления для установки:

   - **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

     Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные программы или чтобы обновить только требуемые программы.

   - **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

     Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

     Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

     Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

     По умолчанию параметр включен.

2. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Закрывать только уязвимости из списка**

     Закрывать только уязвимости, которые выбраны вручную в списке. Этот список

содержит все обнаруженные уязвимости.

Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных программах или чтобы закрыть уязвимости только в требуемых программах.

3. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. В окне **Тип правила** выберите **Правило для обновлений Windows Update**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

   - **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те

обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
3. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновления программ сторонних производителей:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. В окне **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен

или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

## См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

## Создание задачи Установка обновлений Центра обновления Windows

Задача *Установка обновлений Центра обновления Windows* позволяет устанавливать обновления программного обеспечения, предоставляемые службой Центра обновления Windows, на управляемые устройства.

Если у вас нет лицензии на Системное администрирование (см. стр. 353), вы не можете создавать задачи с типом *Установка обновлений Центра обновления Windows*. Чтобы установить новые обновления, вы можете добавить их в существующую задачу *Установка обновлений Центра обновления Windows*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295) вместо задачи *Установка обновлений Центра обновления Windows*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами (см. стр. 1299). Также эта задача позволяет устанавливать обновления для программ сторонних производителей, то есть программ производства не Microsoft.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

► *Чтобы создать задачу Установка обновлений Центра обновления Windows:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для программы Kaspersky Security Center выберите тип задачи **Установка обновлений Центра обновления Windows**.

4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.

   Откроется список обновлений.

7. Выберите обновления Центра обновлений Windows, которые вы хотите установить и нажмите на кнопку **ОК**.
8. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Запрашивать у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

     По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

     Если параметр выключен, предложение перезагрузки отображается только один раз.

   - **Принудительно перезагрузить через (мин)**

     После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

     По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

   - **Принудительно закрывать программы в заблокированных сеансах**

Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. Задайте параметры учетной записи:
   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

     По умолчанию выбран этот вариант.
   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.
   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.
   - **Пароль**

     Пароль учетной записи, от имени которой будет запускаться задача.
2. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
3. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
4. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
5. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.
6. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

## Просмотр информации о доступных обновлениях программ сторонних производителей

Вы можете просмотреть список доступных обновлений для программ сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

► *Чтобы просмотреть список доступных обновлений для программ сторонних производителей, установленных на клиентских устройствах,*

В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений программ. Нажмите на значок **Фильтр** (  ) в верхнем правом углу списка обновлений программ для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в программах.

► *Чтобы просмотреть свойства обновления:*

1. Нажмите на имя требуемого обновления программного обеспечения.
2. Откроется окно свойств обновления, в котором отображается следующая информация, сгруппированная по закладкам:
   - **Общие**
   - **Атрибуты**
   - **Устройства**
   - **Закрываемые уязвимости**
   - **Пересечения обновлений**
   - **Задачи для установки обновления**

► *Чтобы просмотреть статистику установки обновления:*

1. Установите флажок рядом с требуемым обновлением.
2. Нажмите на кнопку **Статистика состояния установки обновлений**.

На диаграмме отобразится информация о статусах обновлений. Нажав на статус, откроется список устройств, на которых обновление имеет выбранный статус.

Вы можете просмотреть информацию о доступных обновлениях для программ сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранном управляемом устройстве под управлением Windows.

► *Чтобы просмотреть список доступных обновлений для программ сторонних производителей, установленных на выбранном управляемом устройстве:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.
2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления программ сторонних производителей.

   Откроется окно свойств выбранного устройства.
3. В окне свойств выбранного устройства выберите закладку **Дополнительно**.
4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, установите флажок **Показывать установленные обновления**.

Отобразится список доступных обновлений программ сторонних производителей для выбранного устройства.

## См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

## Экспорт списка доступных обновлений в файл

Вы можете экспортировать отображаемый список обновлений для программ сторонних производителей, включая программное обеспечение Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

► *Чтобы экспортировать список доступных обновлений для программ сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:*

1. В главном окне программы перейдите в раздел **Операции → Управление патчами → Обновления программного обеспечения**.

   На странице отображается список доступных обновлений для программ сторонних производителей, установленных на всех управляемых устройствах.

2. Нажмите на кнопку **Экспортировать строки в файл формата TXT** или **Экспортировать строки в файл формата CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список доступных обновлений для программ сторонних производителей, включая программное обеспечение Microsoft, загружается на устройство, которое вы используете в данный момент.

► *Чтобы экспортировать список доступных обновлений для программ сторонних производителей в текстовый файл, установленных на выбранном управляемом устройстве:*

1. Откройте список доступных обновлений программ сторонних производителей на выбранном управляемом устройстве (см. стр. 1305).
2. Выберите обновления программного обеспечения, которые вы хотите экспортировать.

   Пропустите этот шаг, если вы хотите экспортировать полный список обновлений программ.

   При экспорте полного списка обновлений программ, будут экспортированы только те обновления, которые отображаются на текущей странице.

   Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

3. Нажмите на кнопку **Экспортировать строки в файл формата TXT** или **Экспортировать строки в файл формата CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список обновления программ сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранных управляемых устройствах, загружается на устройство, которое вы используете в данный момент.

См. также:

Сценарий:Обновление программ сторонних производителей .....489

## Одобрение и отклонение обновлений программ сторонних производителей

При настройке задачи *Установка требуемых обновлений и закрытия уязвимостей*, вы можете создать правило, для выполнения которого устанавливаемые обновления должны иметь определенный статус. Например, правило обновления может разрешить установку следующего:

- только одобренных обновлений;
- только одобренных обновлений и неопределенных обновлений;
- всех обновлений, независимо от статусов обновлений.

Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. При ручном одобрении большого количества обновлений производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.
2. Выберите обновления, которые требуется подтвердить или отклонить.
3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

► *Чтобы одобрить или отклонить обновление:*

1. В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.
2. Выберите обновление, которое требуется одобрить или отклонить.

   Откроется окно свойств обновления.
3. В разделе **Общие** выберите статус обновления, изменив параметр **Статус одобрения обновления**. Вы можете выбрать статус *Одобрено*, *Отклонено* или *Не определено*.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранные обновления имеют статусы, которые вы указали.

Если вы устанавливаете статус **Отклонено** для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить их, вы можете сделать это вручную локально.

См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Создание задачи Установка требуемых обновлений и закрытие уязвимостей ..... 1295

## Создание задачи Синхронизация обновлений Windows Update.

Задача *Синхронизация обновлений Windows Update* доступна при наличии лицензии на Системное администрирование (см. стр. 353).

Задача *Синхронизация обновлений Windows Update* требуется, если вы хотите использовать Сервер администрирования в роли WSUS-сервера. В этом случае Сервер администрирования загружает обновления Windows в базу данных и предоставляет обновления Центра обновления Windows на клиентских устройствах в централизованном режиме с помощью Агентов администрирования. Если в сети не используется WSUS-сервер, то каждое клиентское устройство самостоятельно загружает обновления Microsoft с внешних серверов.

Задача *Синхронизация обновлений Windows Update* загружает с серверов Microsoft только метаданные. Во время выполнения задачи установки обновлений, Kaspersky Security Center загружает только те обновления, которые вы выбрали для установки.

Во время выполнения задачи **Синхронизация обновлений Windows Update**, программа получает список актуальных обновлений с сервера обновлений Microsoft. После чего Kaspersky Security Center определяет список устаревших обновлений. При следующем запуске задачи **Поиск уязвимостей и требуемых обновлений** Kaspersky Security Center отмечает устаревшие обновления и устанавливает время на удаление. При следующем запуске задачи **Синхронизация обновлений Windows Update** удаляются обновления, которые были отмечены на удаление 30 дней назад. Kaspersky Security Center также выполняет дополнительную проверку для удаления устаревших обновлений, которые были отмечены на удаление более 180 дней назад.

После завершения работы задачи **Синхронизация обновлений Windows Update** и удаления устаревших обновлений в базе данных могут оставаться хеш-коды файлов удаленных обновлений, а также соответствующие им файлы в папке %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles, в случае если они были загружены ранее. С помощью задачи **Обслуживание Сервера администрирования** (см. стр. 870) можно удалить такие устаревшие записи из базы данных и соответствующих им файлов.

► *Чтобы создать задачу Синхронизация обновлений Windows Update:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для программы Kaspersky Security Center выберите тип задачи **Синхронизация обновлений Windows Update**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Включите параметр **Загрузить файлы экспресс-установки**, если вы хотите, чтобы файлы экспресс-обновления загружались при выполнении задачи.

   Когда Kaspersky Security Center синхронизирует обновления с серверами Microsoft Windows Update Servers, информация обо всех файлах сохраняется в базе данных Сервера администрирования. Также на диск загружаются все файлы, необходимые для обновления, при взаимодействии с Агентом обновления Windows. В частности, Kaspersky Security Center сохраняет информацию о файлах экспресс-установки в базу данных и загружает их по мере необходимости. Загрузка файлов экспресс-установки приводит к сокращению свободного места на диске.

   Чтобы уменьшить сокращение объема дискового пространства и снизить трафик, выключите параметр **Загрузить файлы экспресс-установки**.
6. Выберите программы, для которых требуется загрузить обновления.

   Если установлен флажок **Все программы**, то обновления будут загружаться для всех имеющихся программ, а также для тех программ, которые могут быть выпущены в будущем.
7. Выберите категории обновлений, которые вы хотите загрузить на Сервер администрирования.

   Если установлен флажок **Все категории**, то обновления будут загружаться для всех имеющихся категорий обновлений, а также для тех категорий, которые могут появиться в будущем.
8. Выберите языки локализации обновлений, которые вы хотите загрузить на Сервер администрирования. Выберите один из следующих вариантов:

   - **Загружать все языки, включая новые**

     Если выбран этот вариант, на Сервер администрирования будут загружаться все доступные языки локализации обновлений. По умолчанию выбран этот вариант.

   - **Загружать выбранные языки**

     Если выбран этот вариант, в списке можно выбрать языки локализации обновлений, которые должны загружаться на Сервер администрирования.
9. Укажите, под какой учетной записью запускать задачу. Выберите один из следующих вариантов:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

     По умолчанию выбран этот вариант.

   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.
10. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.

14. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

Сценарий:Обновление программ сторонних производителей .....489

## Автоматическое обновление программ сторонних производителей

Некоторые программы сторонних производителей могут обновляться автоматически. Поставщик программы определяет, поддерживает ли программа функцию автоматического обновления. Если программа стороннего производителя, установленная на управляемом устройстве, поддерживает автоматическое обновление, вы можете указать параметр автоматического обновления в свойствах программы. После изменения параметра автоматического обновления Агенты администрирования применяют новый параметр на каждом управляемом устройстве, на котором установлена программа.

Параметр автоматического обновления не зависит от других объектов и возможностей Системного администрирования. Например, этот параметр не зависит от статуса одобрения обновления или задач установки обновления, таких как *Установка требуемых обновлений и закрытие уязвимостей*, *Установка обновлений Центра обновления Windows*, and *Закрытие уязвимостей*.

► *Чтобы настроить параметр автоматического обновления для программы стороннего производителя:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Реестр программ**.

2. Нажмите на имя программы, для которой вы хотите изменить параметр автоматического обновления.

   Чтобы упростить поиск, вы можете отфильтровать список по графе **Статус автоматических обновлений**.

   Откроется окно свойств программы.

3. В разделе **Общие** выберите значение для следующего параметра:

   **Статус автоматических обновлений**

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка автоматического обновления применяется к выбранной программе.

### См. также:

Сценарий:Обновление программ сторонних производителей .....489

kaspersky

# Закрытие уязвимостей в программах сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center связанные с закрытием уязвимостей в программах, установленных на управляемых устройствах.

## В этом разделе



## Сценарий: Обнаружение и закрытие уязвимостей в программах сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционных системах, в программах сторонних производителей, включая программы Microsoft (см. стр. 1275).

### Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в программах Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в программах сторонних производителей, отличных от программ Microsoft.

### Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

a. **Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах**

Чтобы найти уязвимости в программах, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную.

Инструкции:

- Консоль администрирования: Консоль администрирования: Поиск уязвимостей и требуемых обновлений (см. стр. 522), Настройка расписания задачи Поиск уязвимостей и требуемых обновлений (см. стр. 409).
- Kaspersky Security Center 14.2 Web Console: Создание задачи Поиск уязвимостей и требуемых обновлений (см. стр. 1289), Параметры задачи поиска уязвимостей и требуемых обновлений (см. стр. 1292).

**b. Анализ списка обнаруженных уязвимостей в программах**

Просмотрите список **Уязвимости в программах** и решите, какие уязвимости требуется закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах.

Инструкции:

- Консоль администрирования: Просмотр информации об уязвимостях в программах (см. стр. 520), Просмотр статистики уязвимостей на управляемых устройствах (см. стр. 521).
- Kaspersky Security Center 14.2 Web Console: Просмотр информации об уязвимостях в программах (см. стр. 1331), Просмотр статистики уязвимостей на управляемых устройствах (см. стр. 1333).

**c. Настройка закрытия уязвимостей**

Обнаружив уязвимости в программах, вы можете закрыть уязвимости в программах на управляемых устройствах, используя задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295) или задачу *Закрытие уязвимостей* (см. стр. 1320).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в программах сторонних производителей, включая программы Microsoft, установленные на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Для закрытия уязвимостей в программах в задаче *Установка требуемых обновлений и закрытия уязвимостей* используются рекомендуемые обновления программного обеспечения.

Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в программах сторонних производителей, которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления программ Microsoft и пользовательские исправления для программ сторонних производителей.

Вы можете запустить мастер закрытия уязвимостей, который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

Инструкции:

- Консоль администрирования: Пользовательские исправления для уязвимостей в программах сторонних производителей (см. стр. 549), Закрытие уязвимостей в программах (см. стр. 527).
- Kaspersky Security Center 14.2 Web Console: Пользовательские исправления для уязвимостей в программах сторонних производителей (см. стр. 1330), Закрытие уязвимостей в программах сторонних производителей (см. стр. 1316), Создание задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295).

**d. Задание расписания задачи**

Чтобы убедится, что список уязвимостей всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. Рекомендуемый средний период – один раз в неделю.

Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью или реже, что и запуск задачи *Поиск уязвимостей и требуемых обновлений*. При задании расписания задачи *Закрытие уязвимостей* вы должны выбрать исправления программ Microsoft или указать пользовательские исправления для программ сторонних производителей каждый раз перед запуском задачи.

При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

**e. Игнорирование уязвимостей в программах (если требуется)**

Вы можете игнорировать уязвимости в программах, которые должны быть закрыты на всех управляемых устройствах или только на выбранных управляемых устройствах.

Инструкции:

- Консоль администрирования: Игнорирование уязвимостей в программах (см. стр. 548)
- Kaspersky Security Center 14.2 Web Console: Игнорирование уязвимостей в программах (см. стр. 1334)

**f. Запуск задачи закрытия уязвимости**

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

**g. Создание отчета о результатах закрытия уязвимостей в программах (если требуется)**

Чтобы просмотреть статистику о закрытии уязвимостей, сформируйте отчет об уязвимостях. В отчете отображается информация об уязвимостях в программах, которые не закрыты. Таким образом, вы можете иметь представление об обнаружении и закрытии уязвимостей в программах сторонних производителей в вашей организации, включая программное обеспечение Microsoft.

Инструкции:

- Консоль администрирования: Создание и просмотр отчета (см. стр. 588)
- Kaspersky Security Center 14.2 Web Console: Генерация и просмотр отчета (см. стр. 1372)

**h. Проверка настройки обнаружения и закрытия уязвимостей в программах сторонних производителей**

Убедитесь, что вы выполнили следующее:

- обнаружили и просмотрели список уязвимостей в программах на управляемых устройствах;
- игнорировали уязвимости в программах, если хотели;
- настроили задачу закрытия уязвимости;

- запланировали запуск задач для поиска и закрытия уязвимостей в программах так, чтобы они запускались последовательно;
- проверили, что задача закрытия уязвимостей была запущена.

**Результаты**

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске задачи, задача выполняет сопоставление списка доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в правилах, будут загружены в хранилище Сервера администрирования и будут установлены для закрытия уязвимостей в программах.

Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в программах Microsoft.

См. также:

О программах сторонних производителей .....1275

## Об обнаружении и закрытии уязвимостей в программах

Kaspersky Security Center обнаруживает и закрывает уязвимости в программах на управляемых устройствах под управлением операционных систем семейства Microsoft Windows. Уязвимости обнаруживаются в операционных системах и в программах сторонних производителей, включая программное обеспечение Microsoft (см. стр. 1275).

### Обнаружение уязвимостей в программах

Для обнаружения уязвимостей Kaspersky Security Center выполняет поиск известных уязвимостей программного обеспечения на основе признаков из баз данных об известных уязвимостях. Эта база формируются специалистами "Лаборатории Касперского". Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей, уровень критичности уязвимостей. Вы можете получить сведения об уязвимостях в программах на сайте "Лаборатории Касперского" (https://threats.kaspersky.com/en/).

Kaspersky Security Center использует задачу *Поиск уязвимостей и требуемых обновлений* для поиска уязвимостей в программах.

### Закрытие уязвимостей в программах

Для закрытия уязвимостей в программах, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения следующих задач:

- *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для программ "Лаборатории Касперского" и программ сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Задача загрузки обновлений в хранилище Сервера администрирования (см. стр. 1244) может быть создана вручную.
- *Синхронизация обновлений Windows Update*. Эта задача предназначена для загрузки метаданных обновлений программного обеспечения Microsoft.

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости

программного обеспечения, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, для закрытия уязвимости в программах используйте задачу *Установка требуемых обновлений и закрытия уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, для закрытия уязвимостей используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для программ Microsoft и пользовательских исправлений для программ сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений программ сторонних производителей, которые можно установить с помощью Системного администрирования. Кроме того, специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях, и не проводят другие виды анализа упомянутых выше обновлений.

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

Для закрытия некоторых уязвимостей программного обеспечения вы должны принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Закрытие уязвимостей в программах сторонних производителей

После получения списка уязвимостей в программах вы можете закрыть уязвимости в программах на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в операционной системе и программах сторонних производителей, включая программное обеспечение Microsoft, создав и запустив задачу *Закрыть уязвимости* (см. стр. 1320) или задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295).

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в программах следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.

  В результате создается задача закрытия уязвимостей в программах. Также можно добавить выбранные уязвимости в существующую задачу.

- Запустите мастер закрытия уязвимостей.

  Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование (см. стр. 353).

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач, содержащих те же обновления для установки.

**Закрытие уязвимостей в программах с помощью списка уязвимостей**

► *Чтобы закрыть уязвимости в программах:*

1. Откройте один из списков уязвимостей:
   - Чтобы открыть общий список уязвимостей, в главном меню перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в программах**.
   - Чтобы открыть список уязвимостей управляемого устройства, в главном меню перейдите в раздел **Устройства** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Уязвимости в программах.**
   - Чтобы открыть список уязвимостей для требуемой программы, в главном меню перейдите в раздел **Операции** → **Программы сторонних производителей** → **Реестр программ** → <имя программы> → **Уязвимости**.

   Отобразится страница со списком уязвимостей в программах сторонних производителей.
2. Выберите одну или несколько уязвимостей в списке и нажмите на кнопку **Закрыть уязвимость**.

   Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

   Для закрытия некоторых уязвимостей программного обеспечения вы должны принять Лицензионное соглашение для установки программного обеспечения, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в программном обеспечении не закроется.
3. Выберите один из следующих вариантов:
   - **Новая задача**

     Запустится мастер создания задачи (см. стр. 1111). Если у вас есть лицензия на Системное администрирование (см. стр. 353), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.

- **Закрыть уязвимость (добавить правило в указанную задачу)**

  Выберите задачу, в которую вы хотите добавить выбранные уязвимости. Если у вас есть лицензия на Системное администрирование (см. стр. 353), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу будет автоматически добавлено новое правило для закрытия выбранных уязвимостей. Если у вас нет лицензии, выберите задачу *Закрытие уязвимостей*. Выбранные уязвимости будут добавлены в свойства задачи.

  Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Устройства → Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости программ сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вы должны вручную указать обновления программного обеспечения для закрытия уязвимостей, перечисленных в свойствах задачи.

**Закрытие уязвимостей в программах с помощью мастера закрытия уязвимостей**

Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование (см. стр. 353).

► *Чтобы закрыть уязвимости в программах с помощью мастера закрытия уязвимостей:*

1. В главном окне программы перейдите в раздел **Операции → Управление патчами → Уязвимости в программах**.

   Откроется страница со списком уязвимостей в программах сторонних производителей, установленных на управляемых устройствах.

2. Установите флажок напротив уязвимости, которую требуется закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Откроется мастер закрытия уязвимости. На странице **Выбор задачи закрытия уязвимости** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытия уязвимостей.*
   - *Установка обновлений Центра обновления Windows.*
   - *Закрытие уязвимостей.*

   Вы не можете изменить последние два типа задач для установки новых обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, которые закрывают выбранную уязвимость**.
5. Выберите действие, которое хотите выполнить:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.

- Чтобы добавить новое правило в существующую задачу:
  a. Установите флажок рядом с именем задачи и нажмите на кнопку **Добавить правило**.
  b. На открывшейся странице настройте новое правило:
     - **Правило закрытия уязвимостей данного уровня критичности**
     - **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости** (доступно только для уязвимостей в программах Microsoft)
     - **Правило закрытия уязвимостей в программах выбранного поставщика** (доступно только для уязвимостей в программах сторонних производителей)
     - **Правило закрытия уязвимости во всех версиях выбранной программы** (доступно только для уязвимостей в программах сторонних производителей)
     - **Правило для закрытия выбранной уязвимости**
     - **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

  a. Нажмите на кнопку **Добавить**.

- Чтобы создать задачу:
  a. Нажмите на кнопку **Новая задача**.
  b. На открывшейся странице настройте новое правило:
     - **Правило закрытия уязвимостей данного уровня критичности**
     - **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости** (доступно только для уязвимостей в программах Microsoft)
     - **Правило закрытия уязвимостей в программах выбранного поставщика** (доступно только для уязвимостей в программах сторонних производителей)
     - **Правило закрытия уязвимости во всех версиях выбранной программы** (доступно только для уязвимостей в программах сторонних производителей)
     - **Правило для закрытия выбранной уязвимости**
     - **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

  a. Нажмите на кнопку **Добавить**.

Если вы решили запустить задачу, вы можете закрыть мастер. Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.

Если вы выбрали добавление правила к существующей задаче, откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы решили создать задачу, создайте ее с помощью (см. стр. 1295) мастера создания задачи. Новое правило, добавленное вами в мастер закрытия уязвимостей, отображается в мастере создания задачи. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

## См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в программах на управляемых устройствах с операционными системами Windows. Вы можете закрыть уязвимости в программах сторонних производителей, включая программное обеспечение Microsoft.

Если у вас нет лицензии на Системное администрирование (см. стр. 353), вы не можете создавать задачи с типом *Закрытие уязвимостей*. Чтобы закрыть новые уязвимости, вы можете добавить их в существующую задачу *Закрытие уязвимостей*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 1295) вместо задачи *Закрыть уязвимости*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами (см. стр. 1299).

Вмешательство пользователя может потребоваться при обновлении программ сторонних производителей или при закрытии уязвимостей в программах сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть программу стороннего производителя.

► *Чтобы создать задачу Закрытие уязвимостей:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для программы Kaspersky Security Center выберите тип задачи **Закрытие уязвимостей**.
4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Нажмите на кнопку **Добавить**.

   Откроется список уязвимостей.
7. Выберите уязвимости, которые вы хотите закрыть и нажмите на кнопку **ОК**.

   Для уязвимостей программного обеспечения Microsoft обычно существуют рекомендуемые исправления. Дополнительные действия для них не требуются. Для уязвимостей в программах сторонних производителей сначала необходимо указать исправление пользователя для каждой уязвимости (см. стр. 1330), которую вы хотите закрыть. После этого вы сможете добавить эти уязвимости в задачу *Закрытие уязвимостей*.
8. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать программы в заблокированных сеансах**

  Запущенные программы могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, программа не позволяет перезагрузить устройство.

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

1. Задайте параметры учетной записи:
   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

     По умолчанию выбран этот вариант.
   - **Задать учетную запись**

     В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.
   - **Учетная запись**

     Учетная запись, от имени которой будет запускаться задача.
   - **Пароль**

     Пароль учетной записи, от имени которой будет запускаться задача.
2. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
3. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
4. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
5. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.
6. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

## Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование(см. стр. 353).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в программах сторонних производителей, включая программы Microsoft, установленные на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений (см. стр. 1285) или мастер закрытия уязвимостей (см. стр. 1316).
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.

- Добавьте правило для установки обновлений (см. стр. 1299) в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

► *Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для программы Kaspersky Security Center выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права (см. стр. 1192)**Чтение**, **Изменение** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование**. Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите правила для установки обновления (см. стр. 1299), а затем следующие параметры:

   - **Начинать установку в момент перезагрузки или выключения устройства**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.

   - **Устанавливать необходимые общесистемные компоненты**

     Если флажок установлен, перед установкой обновления программа автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться обновления операционной системы.

     Если этот параметр выключен, необходимо установить пререквизиты вручную.

     По умолчанию параметр выключен.

   - **Разрешать установку новой версии программы при обновлении**

     Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии программы.

     Если этот параметр выключен, программа не обновляется. Можно позднее установить новые версии программ вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию программы или если требуется проверить обновление в тестовой инфраструктуре.

     По умолчанию параметр включен.

После установки новой версии программы может быть нарушена работа других программ, установленных на клиентских устройствах и зависящих от работы обновляемой программы.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, программа загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Папка для загрузки обновлений**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Папка для загрузки обновлений**

Эта папка используется для загрузки обновлений сторонних программ (программ, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики (см. стр. 735), с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

1. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Запрашивать у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, программа с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, программа выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием программы в заблокированных сессиях через (мин)**

  Принудительное завершение работы программ, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа программ на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа программ на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

2. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями

параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.

3. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

4. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
5. В окне свойств задачи укажите общие параметры задачи (см. стр. 1112) в соответствии с вашими требованиями.
6. Нажмите на кнопку **Сохранить**.

   Задача создана и настроена.

Если результаты задачи содержат предупреждение об ошибке 0x80240033 "Windows Update Agent error 80240033 ("License terms could not be downloaded.")", решить эту проблему можно с помощью реестра Windows.

### См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

Об обновлениях программ сторонних производителей ..... 1284

## Добавление правил для установки обновлений

Эта функциональность доступна при наличии лицензии на Системное администрирование (см. стр. 353).

При установке обновлений программного обеспечения или закрытии уязвимостей в программах с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений программ сторонних производителей (то есть программ производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления программ сторонних производителей вы можете выбрать программы и версии программ, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые необходимо закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи Установка требуемых обновлений и закрытие уязвимостей (см. стр. 1295).
- Добавить правило на закладке **Параметры программы** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- С помощью мастера установки обновлений (см. стр. 1285) или мастера закрытия уязвимостей (см. стр. 1316).

► Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. В окне **Тип правила** выберите **Правило для всех обновлений**.
3. В окне **Общие критерии** в раскрывающемся списке укажите следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Обновления** выберите обновления для установки:

   - **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

     Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные программы или чтобы обновить только требуемые программы.

- **Автоматически устанавливать все предыдущие обновления программ, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий программ, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии программ. Выключите этот параметр, если вы хотите непосредственно обновить программы, не пытаясь последовательно установить версии программ. Если установка выбранных обновлений невозможна без установки предыдущих версий программы, обновление программы завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 программы, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

1. В окне **Уязвимости** выберите уязвимости, которые будут закрыты с установкой указанного обновления:

   - **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости программного обеспечения, соответствующие критериям, указанным в окне мастера **Общие критерии**. Выбрано по умолчанию.

   - **Закрывать только уязвимости из списка**

     Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

     Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных программах или чтобы закрыть уязвимости только в требуемых программах.

1. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. В окне **Тип правила** выберите **Правило для обновлений Windows Update**.
3. В окне **Общие условия** настройте следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае

устанавливаются только одобренные обновления.

- **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
- **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
3. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

► Чтобы добавить правило для обновления программ сторонних производителей:

1. Нажмите на кнопку **Добавить**.

Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. В окне **Тип правила** выберите **Правило для сторонних обновлений**.
3. В окне **Общие условия** настройте следующие параметры:
   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.
   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

     Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **Программы** выберите программы и версии программ, для которых вы хотите установить обновления. По умолчанию выбраны все программы.
2. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе Параметры, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

## См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей ..... 516

## Пользовательские исправления для уязвимостей в программах сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в программах сторонних производителей, перечисленные в

параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления программ Microsoft и пользовательские исправления для других программ сторонних производителей. *Пользовательские исправления* это обновления программного обеспечения для закрытия уязвимостей, которые администратор вручную указывает для установки.

► *Чтобы выбрать пользовательские исправления для уязвимостей в программах сторонних производителей:*

1. В главном окне программы перейдите в раздел **Операции → Управление патчами → Уязвимости в программах**.

   На странице отображается список уязвимостей в программах, обнаруженных на клиентских устройствах.

2. В списке уязвимостей в программах перейдите по ссылке с названием уязвимости, для которой вы хотите указать пользовательское исправление.

   Откроется окно свойств уязвимости.

3. На левой панели выберите раздел **Пользовательские и другие исправления**.

   Отобразится список пользовательских исправлений для выбранной уязвимости в программах.

4. Нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку на закладке **Операции → Хранилища → Инсталляционные пакеты**. Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для уязвимости программах сторонних производителей.

6. Нажмите на кнопку **Сохранить**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в программах. После запуска задачи *Закрытие уязвимостей* будет установлен инсталляционный пакет и закрыта уязвимость в программах.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Просмотр информации об уязвимостях в программах, обнаруженных на всех управляемых устройствах

После проверки программного обеспечения на управляемых устройствах на наличие уязвимостей (см. стр. 1289) вы можете просмотреть список уязвимостей в программах, обнаруженных на всех управляемых устройствах.

► *Чтобы просмотреть список уязвимостей в программах, обнаруженных на всех управляемых устройствах,*

В главном окне программы перейдите в раздел **Операции → Управление патчами → Уязвимости в программах**.

На странице отображается список уязвимостей в программах, обнаруженных на клиентских устройствах.

Вы также можете сформировать и просмотреть Отчет об уязвимостях (см. стр. 1372).

Вы можете указать фильтр для просмотра списка уязвимостей в программах. Нажмите на значок **Фильтр** (  ) в верхнем правом углу списка уязвимостей в программах для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в программах.

Вы можете получить подробную информацию о любой уязвимости из списка.

► *Чтобы получить информацию об уязвимости в программах,*

в списке уязвимостей в программах перейдите по ссылке с названием уязвимости.

Откроется окно свойств уязвимости в программах.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Просмотр информации об уязвимостях в программах, обнаруженных на выбранных управляемых устройствах

Вы можете просмотреть информацию об уязвимостях в программах, обнаруженных на выбранном управляемом устройстве под управлением Windows.

► *Чтобы просмотреть список уязвимостей в программах, обнаруженных на выбранном управляемом устройстве:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в программах.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите закладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в программах**.

   Если вы хотите просматривать только те уязвимости, которые можно закрыть, установите флажок **Показывать только те уязвимости, которые можно закрыть**.

Отобразится список уязвимостей в программах, обнаруженных на выбранном управляемом устройстве.

► *Чтобы просмотреть свойства выбранной уязвимости в программах,*

перейдите по ссылке с названием уязвимости в списке уязвимостей в программах.

Откроется окно свойств выбранной уязвимости в программах.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

kaspersky

## Просмотр статистики уязвимостей на управляемых устройствах

Вы можете просмотреть статистическую информацию каждой уязвимости в программах на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на: <количество устройств>*. Статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на: <количество устройств>*. Статус присваивается, если задача закрытия уязвимости успешно завершена.
- *Запланирована к закрытию на: <количество устройств>*. Статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на: <количество устройств>*. Статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требует закрытия на: <количество устройств>*. Статус присваивается, если уязвимость была закрыта только на части управляемых устройств, и ее необходимо закрыть на остальных управляемых устройствах.

► *Чтобы просмотреть статистику уязвимости на управляемых устройствах:*

1. В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в программах**.

   Отобразится страница со списком уязвимостей в программах, обнаруженных на управляемых устройствах.
2. Установите флажок рядом с требуемой уязвимостью.
3. Нажмите на кнопку **Статистика уязвимостей на устройствах**.

Отобразится диаграмма статусов уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Экспорт списка уязвимостей в программах в текстовый файл

Вы можете экспортировать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

► *Чтобы экспортировать список уязвимостей в программах, обнаруженных на всех управляемых устройствах, в текстовый файл:*

1. В главном окне программы перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в программах**.

   Отобразится страница со списком уязвимостей в программах, обнаруженных на управляемых устройствах.

2. Нажмите на кнопку **Экспортировать строки в файл формата TXT** или **Экспортировать строки в файл формата CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в программах, загружается на устройство, которое вы используете в данный момент.

► *Чтобы экспортировать список уязвимостей в программах, обнаруженных на выбранных управляемых устройствах, в текстовый файл:*

1. Откройте список уязвимостей в программах, обнаруженных на выбранном управляемом устройстве (см. стр. 1332).
2. Выберите уязвимости в программах, которые вы хотите экспортировать.

   Пропустите этот шаг, если вы хотите экспортировать полный список уязвимостей в программах, обнаруженных на управляемых устройствах.

   При экспорте полного списка уязвимостей в программах, обнаруженных на управляемом устройстве, будут экспортированы только те уязвимости, которые отображаются на текущей странице.
3. Нажмите на кнопку **Экспортировать строки в файл формата TXT** или **Экспортировать строки в файл формата CSV**, в зависимости от формата, который вы хотите экспортировать.

Файл, содержащий список уязвимостей в программах, экспортируется с выбранного управляемого устройства, которое вы используете в данный момент.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Игнорирование уязвимостей в программах

Вы можете игнорировать уязвимости в программах и не закрывать их. Причины для игнорирования уязвимостей в программах могут быть, например, следующими:

- Вы не считаете уязвимость в программе критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в программах может повредить данные программы, для которой требуется закрыть уязвимость.
- Вы уверены, что уязвимость в программах не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в программах на всех управляемых устройствах или только на выбранных управляемых устройствах.

► *Чтобы пропустить уязвимость в программах на всех управляемых устройствах:*

1. В главном окне программы перейдите в раздел **Операции → Управление патчами → Уязвимости в программах**.

   На странице отображается список уязвимостей в программах, обнаруженных на управляемых устройствах.
2. В списке уязвимостей в программах нажмите на имя уязвимости в программах, которую вы хотите пропустить.

   Откроется окно свойств уязвимости в программах.

3. На закладке **Общие** включите параметр **Игнорировать уязвимость**.
4. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в программах закроется.

Уязвимость в программах пропускается на всех управляемых устройствах.

► *Чтобы пропустить уязвимость в программах на выбранных управляемых устройствах:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.
2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в программах.

   Откроется окно свойств устройства.
3. В окне свойств устройства выберите раздел **Дополнительно**.
4. На левой панели выберите раздел **Уязвимости в программах**.

   Отобразится список уязвимостей в программах, обнаруженных на устройстве.
5. В списке уязвимостей в программах выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

   Откроется окно свойств уязвимости в программах.
6. В окне свойств уязвимости в программах на закладке **Общие** включите параметр **Игнорировать уязвимость**.
7. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в программах закроется.
8. Закройте окно свойств устройства.

Уязвимость в программах пропускается на выбранном устройстве.

Пропущенная уязвимость в программах не будет закрыта после завершения задачи *Закрытие уязвимостей* или *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в программах из списка уязвимостей с помощью фильтра.

### См. также:

Сценарий:Обнаружение и закрытие уязвимостей в программах сторонних производителей .....516

## Управление запуском программ на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center связанные с управлением программ, запущенных на клиентских устройствах.

kaspersky

## В этом разделе



## Сценарий: Управление программами

Вы можете управлять запуском программ на пользовательских устройствах. Вы можете разрешить или запретить запуск программ на управляемых устройствах. Эта функциональность реализуется компонентом Контроль программ. Вы можете управлять программами, установленными на устройствах под управлением Windows или Linux.

Для операционных систем на базе Linux компонент Контроль программ доступен, начиная с версии Kaspersky Endpoint Security 11.2 для Linux.

### Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux создана и активна.

### Этапы

Сценарий использования компонента Контроль программ состоит из следующих этапов:

**a. Формирование и просмотр списка программ на клиентских устройствах**

Этот этап помогает вам определить, какие программы установлены на управляемых устройствах. Вы можете просмотреть список программ и решить, какие программы вы хотите разрешить, а какие запретить, в соответствии с политиками безопасности вашей организации. Ограничения могут быть связаны с политиками информационной безопасности в вашей организации. Вы можете пропустить этот этап, если точно знаете, какие программы установлены на управляемых устройствах.

Инструкции:

Консоль администрирования: Просмотр реестра программ (см. стр. 569).

Kaspersky Security Center 14.2 Web Console: Получение и просмотр списка программ, установленных на клиентских устройствах (см. стр. 1339)

**b. Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации. Вы можете пропустить этот этап, если точно знаете, какие исполняемые файлы установлены на управляемых устройствах.

Инструкции:

Консоль администрирования: Инвентаризация исполняемых файлов (см. стр. 574).

Kaspersky Security Center 14.2 Web Console: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах (см. стр. 1340)

**c. Создание категорий программ для программ, используемых в вашей организации**

Проанализируйте списки программ и исполняемых файлов, хранящихся на управляемых устройствах. На основании анализа создайте категории программ. Рекомендуется создать категорию "Рабочие программы", которая охватывает стандартный набор программ, используемых в вашей организации. Если разные группы пользователей используют разные наборы программ в своей работе, для каждой группы пользователей можно создать отдельную категорию программ.

В зависимости от набора критериев для создания категории программ вы можете создавать категории программ трех типов.

Инструкции:

Консоль администрирования: Создание пополняемой вручную категории программ (см. стр. 560), Создание категории программ, в которую входят исполняемые файлы с выбранных устройств (см. стр. 562), Создание категории программ, в которую входят исполняемые файлы из выбранных папок (см. стр. 563).

Kaspersky Security Center 14.2 Web Console: Создание пополняемой вручную категории программ (см. стр. 1342), Создание категории программ, в которую входят исполняемые файлы с выбранных устройств (см. стр. 1345), Создание категории программ, в которую входят исполняемые файлы из выбранных папок (см. стр. 1346).

**d. Настройка компонента Контроль программ в политики Kaspersky Endpoint Security**

Настройте компонент Контроль программ в политике Kaspersky Endpoint Security с использованием категорий программ, которые вы создали на предыдущем этапе.

Инструкции:

Консоль администрирования: Настройка управления запуском программ на клиентских устройствах (см. стр. 567).

Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349)

**e. Включение компонента Контроль программ в тестовом режиме**

Чтобы правила Контроля программ не блокировали программы, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля программ и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать программы, запуск которых запрещен правилами Контроля программ, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля программ рекомендуется выполнить следующие действия:

Определите период тестирования. Период тестирования может варьироваться от нескольких дней до двух месяцев.

Изучите события, возникающие в результате тестирования работы компонента Контроль программ.

Инструкции для Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349). Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

**f. Изменение параметров категорий программ компонента Контроль программ**

Если требуется, измените параметры компонента Контроль программ. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль программ, в категорию программ пополняемую вручную.

Инструкции:

Консоль администрирования: Добавление исполняемых файлов, связанных с событием, в категорию программы (см. стр. 565)

Kaspersky Security Center 14.2 Web Console: Добавление исполняемых файлов, связанных с событием, в категорию программы (см. стр. 1351)

**g. Применение правил Контроля программ в рабочем режиме**

После проверки правил Контроля программ и завершения настройки категорий программ вы можете применить правила Контроль программ в рабочем режиме.

Инструкции для Kaspersky Security Center 14.2 Web Console: Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows (см. стр. 1349). Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

**h. Проверка конфигурации Контроля программ**

Убедитесь, что вы выполнили следующее:

Создали категории программ.

Настроили Контроль программ с использованием категорий программ.

Применили правила Контроля программ в рабочем режиме.

**Результаты**

После завершения сценария, запуск программ на управляемых устройствах контролируется. Пользователи могут запускать только те программы, которые разрешены в вашей организации, и не могут запускать программы, запрещенные в вашей организации.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windowshttps://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

## О Контроле программ

Компонент Контроль программ контролирует попытки пользователей запуска программ и регулирует запуск программ с помощью правил Контроля программ.

Компонент Контроль программ доступен для программ Kaspersky Endpoint Security для Windows и Kaspersky Security для виртуальных сред Легкий агент. Все инструкции в этом разделе описывают настройку Контроля программ для программы Kaspersky Endpoint Security для Windows.

Запуск программ, параметры которых не соответствуют ни одному из правил Контроля программ, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех программ, кроме программ, указанных в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите заблокировать запуск всех программ, кроме программ, указанных в разрешающих правилах.

Правила Контроля программ реализуются с помощью категорий программ. Вы создаете категории программ с определенными критериями. В Kaspersky Security Center существует три типа категорий программ:

- Пополняемая вручную категория (см. стр. 1342). Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, KL-категория, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы выбранных устройств (см. стр. 1345). Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок (см. стр. 1346). Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

### См. также:

Сценарий:Управление программами .....556

## Получение и просмотр списка программ, установленных на клиентских устройствах

Kaspersky Security Center выполняет инвентаризацию программного обеспечения, которое установлено на управляемых клиентских устройствах, работающих под управлением операционной системы Linux и Windows.

Агент администрирования составляет список программ, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка программ.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных программах из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных программах Агент администрирования получает от диспетчеров пакетов.

► *Чтобы просмотреть список программ, установленных на управляемых устройствах,*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Реестр программ**.

   На странице отображается таблица с программами, установленными на управляемых устройствах. Выберите программу, чтобы просмотреть свойства этой программы, например: имя производителя, номер версии, список исполняемых файлов, список устройств, на которых установлена программа,

список доступных обновлений программного обеспечения или список обнаруженных уязвимостей программного обеспечения.

2. Вы можете группировать и фильтровать данные таблицы с установленными программами следующим образом:

   - Нажмите на значок параметров ( ) в правом верхнем углу таблицы.

     В открывшемся меню **Параметры граф** выберите столбцы, которые будут отображаться в таблице. Чтобы просмотреть тип операционной системы клиентских устройств, на которых установлена программа, выберите столбец **Тип операционной системы**.

   - Нажмите на значок фильтрации ( ) в правом верхнем углу таблицы, укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица установленных программ.

*Чтобы просмотреть список программ, установленных на выбранном управляемом устройстве,*

В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства** → **<имя устройства>** → **Дополнительно** → **Реестр программ**. В этом меню можно экспортировать список программ в файлы форматов CSV или TXT.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

## См. также:

Сценарий:Управление программами .....556

## Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вы должны создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для следующих программ:

- Kaspersky Endpoint Security для Windows;
- Kaspersky Endpoint Security для Linux.
- Kaspersky Security для виртуальных сред 4.0 Легкий агент и выше;

Вы можете снизить нагрузку на базу данных при получении информации об установленных программах. Для этого рекомендуется запускать задачу инвентаризации на нескольких эталонных устройствах, на которых установлен стандартный набор программ.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:*

1. В главном окне программы перейдите к закладке **Устройства** → **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи (см. стр. 1111). Следуйте далее указаниям мастера.

3. На странице **Новая задача** в выпадающем списке **Программы** выберите Kaspersky Endpoint Security для Windows или Kaspersky Endpoint Security для Linux, в зависимости от типа операционной системы клиентских устройств.

4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в следующих справках:

- Онлайн-справка Kaspersky Endpoint Security для Windows https://help.kaspersky.com/KESWin/11.5.0/ru-RU/
- Онлайн-справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/219385.htm
- Kaspersky Security для виртуальных сред Легкий агент https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, установленных на управляемых устройствах, и вы можете просмотреть этот список.

При выполнении инвентаризации программа обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR, а также HTML-файлы.

► *Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,*

В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

► *Чтобы отправить исполняемый файл управляемого устройства в "Лабораторию Касперского":*

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Исполняемые файлы**.
2. Перейдите по ссылке исполняемого файла, который вы хотите отправить в "Лабораторию Касперского".
3. В открывшемся окне перейдите в раздел **Устройства** и установите флажок рядом с управляемым устройством, с которого вы хотите отправить исполняемый файл.

> Перед отправкой исполняемого файла убедитесь, что управляемое устройство имеет прямое подключение к Серверу администрирования, установив флажок **Не разрывать соединение с Сервером администрирования** (см. стр. 1123).

4. Нажмите на кнопку **Отправить в "Лабораторию Касперского"**.

Выбранный исполняемый файл загружается для дальнейшей отправки в "Лабораторию Касперского".

### См. также:

Сценарий:Управление программами .....556

## Создание пополняемой вручную категории программ

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию программ и использовать ее в настройке компонента Контроль программ.

► *Чтобы создать пополняемую вручную категорию программ:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Категории программ**.

   Откроется страница со списком категорий программ.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Следуйте далее указаниям мастера.

3. На странице мастера **Выбор способа создания категории** выберите параметр **Пополняемая вручную категория**.
4. На странице **Условия** мастера нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.
5. На странице **Критерии условия** выберите тип правила для создания категории из списка:
   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать категорию программ "Лаборатории Касперского". Программы, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию программ.

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

   - **Задайте путь к программе (поддерживаются маски)**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию программ.

   - **Съемный диск**

Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск программы. Программы, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию программ.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:
  - **Выберите из списка исполняемых файлов**

    Если выбран этот вариант, программы для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - **Выберите из реестра программ**

Если выбран этот параметр, отображается реестр программ. Вы можете выбрать программы из реестра и указать следующие метаданные файла:

- Имя файла.
- Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Название программы.
- Версия программы. Вы можете указать точное значение версии или написать условие, например, «больше, чем 5.0».
- Производитель.
  - **Задайте вручную**

    Если выбран этот вариант, вы должны указать хеш файла, метаданные или сертификат в качестве условия добавления программ в пользовательскую категорию.

    **Хеш файла**

    В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

    SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

    Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

    - Если все экземпляры программ безопасности, установленных в вашей сети, являются версиями программы Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA-256**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
    - Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию,

созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.

- Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA-256** и флажок **MD5-хеш**.

**Метаданные**

Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Метаданные будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в категорию программ.

**Сертификат**

Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

- **Из файла MSI-пакета / архивной папки**

  Если выбран этот вариант, в качестве условия добавления программ в пользовательскую категорию можно указать файл установщика MSI. Метаданные установщика программы будут передаваться на Сервер администрирования. Программы, у которых метаданные установщика совпадают с указанным установщиком MSI, будут добавлены в пользовательскую категорию программ.

Выбранный критерий добавлен в список условий.

Вы можете добавить столько критериев для создания категории программ, сколько вам нужно.

1. На странице **Исключения** мастера нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.
2. На странице **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория программ. Оно появится в списке категорий программ. Вы можете создать категорию программ при настройке компонента Контроль программ.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

## См. также:

Сценарий:Управление программами ..... 556

## Создание категории программ, в которую входят исполняемые файлы с выбранных устройств

Вы можете использовать исполняемые файлы с устройства как шаблон исполняемых файлов, запуск которых вы хотите разрешить или запретить. На основе исполняемых файлов с выбранных устройств вы можете создать категорию программ и использовать ее для настройки компонента Контроль программ.

► *Чтобы создать категорию программ, в которую входят исполняемые файлы с выбранных устройств:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Категории программ**.

   Откроется страница со списком категорий программ.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку Далее.

3. На странице **Выбор способа создания категории** мастера, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств**.

4. Нажмите на кнопку **Добавить**.

5. В открывшемся окне выберите устройство или устройства, чьи исполняемые файлы будут использоваться для создания категории программ.

6. Задайте следующие параметры:

   - Алгоритм вычисления хеш-функции

     В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

     SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

     Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

     - Если все экземпляры программ безопасности, установленных в вашей сети, являются версиями программы Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA-256**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.
     - Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для

файлов категории.

Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA-256** и флажок **MD5-хеш**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Синхронизация данных с хранилищем Сервера администрирования**

Выберите этот параметр, если вы хотите, чтобы Сервер администрирования периодически выполнял проверку изменений в указанной папке (или папках).

По умолчанию параметр выключен.

Если вы включите этот параметр, укажите период (в часах), чтобы проверять изменения в указанной папке (папках). По умолчанию период проверки равен 24 часам.

- **Тип файла**

  В этом разделе вы можете указать тип файла, который используется для создания категории программ.

  **Все файлы**. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

  **Только файлы вне категорий программ**. Для создаваемой категории учитываются только файлы вне категорий программ.

- **Папки**

В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории программ.

**Все папки**. Для создаваемой категории учитываются все папки. По умолчанию выбран этот вариант.

**Указанная папка**. Для создаваемой категории учитывается только указанная папка. Если вы выбирали этот параметр, вы должны указать путь к папке.

После завершения мастера создается категория программ. Оно появится в списке категорий программ. Вы можете создать категорию программ при настройке компонента Контроль программ.

## См. также:

Сценарий:Управление программами .....556

## Создание категории программ, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию программ и использовать ее для настройки компонента Контроль программ.

► *Чтобы создать категорию программ, в которую входят исполняемые файлы из выбранных папок:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Категории программ**.

   Откроется страница со списком категорий программ.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На странице **Выбор способа создания категории** мастера, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы из указанной папки.**

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории программ.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию программ включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль программ регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию программ включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - Алгоритм вычисления хеш-функции: **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

     В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center для файлов категории. Информация о вычисленных хеш-функциях хранится в базе данных Сервера администрирования. Хранение хеш-функций увеличивает размер базы данных незначительно.

     SHA-256 – криптографическая хеш-функция, в алгоритме которой не найдено уязвимости, и она считается наиболее надежной криптографической функцией в настоящее время. Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше поддерживают вычисление хеш-функции SHA-256. Вычисление хеш-функции MD5 поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows.

     Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

     - Если все экземпляры программ безопасности, установленных в вашей сети, являются версиями программы Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, установите флажок **SHA-256**. Не рекомендуется добавлять категорию, созданную по критерию SHA-256 исполняемого файла, для версий

программ ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows. Это может привести к сбою программы безопасности. В этом случае вы можете использовать криптографическую хеш-функцию MD5 для файлов категории.

- Если в вашей сети установлены более ранние версии, чем Kaspersky Endpoint Security 10 Service Pack 2 для Windows, выберите **MD5-хеш**. Добавить категорию, созданную по критерию контрольной суммы MD5 исполняемого файла, для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше, нельзя. В этом случае вы можете использовать криптографическую хеш-функцию SHA-256 для файлов категории.

Если разные устройства в вашей сети используют как более ранние, так и более поздние версии Kaspersky Endpoint Security 10, установите флажок **SHA-256** и флажок **MD5-хеш**.

По умолчанию флажок **Вычислять SHA-256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше)** установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, программа периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

После завершения мастера создается категория программ. Оно появится в списке категорий программ. Вы можете использовать категорию программ для настройки компонента Контроль программ.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

## См. также:

Сценарий:Управление программами .....556

## Просмотр списка категорий программ

Вы можете просмотреть список настроенных категорий программ и параметры каждой категории программ.

► *Чтобы просмотреть список категорий программ,*

В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Категории программ**.

Откроется страница со списком категорий программ.

► *Чтобы просмотреть свойства категории программ,*

нажмите на имя категории программ.

Откроется окно свойств выбранной категории программ. Параметры сгруппированы на нескольких закладках.

См. также:

Сценарий:Управление программами .....556

## Настройка компонента Контроль программ в политики Kaspersky Endpoint Security для Windows

После создания категорий для Контроля программ (см. стр. 558), вы можете использовать их для настройки Контроля программ в политиках Kaspersky Endpoint Security для Windows.

► *Чтобы настроить компонент Контроль программ в политике Kaspersky Endpoint Security для Windows:*

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.

   Отобразится страница со списком политик.

2. Нажмите на политику **Kaspersky Endpoint Security для Windows**.

   Откроется окно свойств политики.

3. Перейдите в раздел **Параметры программы → Контроль безопасности → Контроль программ**.

   Отобразится окно **Контроль программ** с параметрами компонента Контроль программ.

4. Параметр **Контроль программ** включен по умолчанию. Убедитесь, что переключатель **Контроль программ Выключен** переведен в неактивное положение.

5. В блоке **Параметры Контроля программ** включите режим работы с применением правил Контроля программ и разрешите Kaspersky Endpoint Security для Windows блокировку запуска программ.

   Если вы хотите протестировать правила Контроля программ, в разделе **Параметры Контроля программ**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security для Windows не блокирует запуск программ, но фиксирует информацию о сработавших правилах в отчете. Перейдите по ссылке **Просмотреть отчет** для просмотра этой информации.

6. Включите параметр **Управление загрузкой модулей DLL**, если вы хотите, чтобы программа Kaspersky Endpoint Security для Windows контролировала загрузку модулей DLL при запуске программ пользователями.

   Информация о модуле и программе, которая загрузила модуль, будет сохранена в отчете.

   Kaspersky Endpoint Security для Windows контролирует только DLL модули и драйверы, которые были загружены после того, как параметр **Управление загрузкой модулей DLL** был включен. Перезагрузите устройство после выбора параметра **Управление загрузкой модулей DLL**, если вы

хотите, чтобы программа Kaspersky Endpoint Security для Windows контролировала все модули и драйверы DLL, включая те, которые были загружены до запуска Kaspersky Endpoint Security для Windows.

7. (Если требуется.) В блоке **Шаблоны сообщений** измените шаблон сообщения, которое отображается, когда программа заблокирована для запуска, и шаблон сообщения электронной почты, которое отправляется вам.
8. В блоке параметров **Режим Контроля программ** выберите режим **Список запрещенных** или **Список разрешенных**.

   По умолчанию выбран режим **Список запрещенных**.
9. Перейдите по ссылке **Параметры списков правил**.

   Откроется окно **Списки запрещенных и разрешенных**, в котором можно добавить категорию программ. По умолчанию отображается закладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается закладка **Список разрешенных**, если выбран режим **Список разрешенных**.
10. В окне **Списки запрещенных и разрешенных** нажмите на кнопку **Добавить**.

    Откроется окно **Правило Контроля программ**.
11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории программ**.
12. Добавьте категорию программ (или категории), которые вы создали ранее.

    Вы можете изменить параметры категории, нажав на кнопку **Изменить**.

    Вы можете создать категорию, нажав на кнопку **Добавить**.

    Вы можете удалить категорию, нажав на кнопку **Удалить**.
13. После того как формирование списка категорий программ завершено, нажмите кнопку **ОК**.

    Окно **Категории программ** закрывается.
14. В окне правил **Контроль программ** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля программ.
15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля программ**.
16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.
17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль программ**.
18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль программ настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/ru-RU/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

kaspersky

См. также:

Сценарий:Управление программами .....556

## Добавление исполняемых файлов, связанных с событием, в категорию программы

После настройки компонента Компонента Контроль программ в политиках Kaspersky Endpoint Security для Windows в списке событий могут отображаться следующие события:

- **Запуск программы запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль программ для применения правил.
- **Запуск программы запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль программ для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска программы** (*Предупреждающее* событие). Это событие отображается, если вы настроили Контроль программ для применения правил, а пользователь запросил доступ к программе, которая заблокирована для запуска.

Рекомендуется создавать выборки событий (см. стр. 1377) для просмотра событий, связанных с компонентом Контроль программ.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля программ, в существующую категорию программ или в новую категорию программ. Вы можете добавлять исполняемые файлы только в категорию программ пополняемую вручную.

► *Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль программ, в категорию программ:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем программ, и запустите формирование этой выборки событий (см. стр. 1378).

   Если вы не создали выборку событий, связанную с Контролем программ, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию программ, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию программ**

       Выберите этот параметр, если вы хотите создать категорию программ на основе исполняемых файлов, связанных с событиями.

       По умолчанию выбран этот вариант.

       Если вы выбрали этот параметр, укажите имя новой категории.

     - **Добавить в существующую категорию**

Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию программ.

По умолчанию вариант не выбран.

Если вы выбрали этот параметр, выберите категорию программ, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

- В блоке **Тип правила** выберите следующие параметры:
  - **Правила для добавления в область действия.**
  - **Правила для добавления в исключения.**
- В разделе **Параметр, используемый в качестве условия** выберите один из следующих параметров:
  - **Данные сертификата (или SHA-256 для файлов без сертификата)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA-256 для файлов без сертификата.

    По умолчанию выбран этот вариант.

  - **Данные сертификата (файлы без сертификата пропускаются)**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

  - **Только SHA-256 (файлы без хеша пропускаются)**

    Каждый файл имеет свою уникальную хеш-функцию SHA-256. При выборе хеш-функции SHA-256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

    Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA-256 исполняемого файла.

  - **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

    Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции MD5 исполняемого файла. Вычисление хеш-функции MD5 поддерживается для версий Kaspersky Endpoint Security 10 Service Pack 1 для Windows и ниже.

5. Нажмите на кнопку **ОК**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля программ, добавляются в существующую категорию программ или в новую категорию программ. Вы можете просмотреть параметры категории программ, которую вы изменили или создали.

Подробную информацию о Контроле программ см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Windows
  https://support.kaspersky.com/KESWin/11.5.0/RU-ru/127971.htm
- Онлайн-справка Kaspersky Endpoint Security для Linux
  https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/
- Онлайн-справка Kaspersky Security для виртуальных сред Легкий агент
  https://support.kaspersky.com/KSVLA/5.2/ru-RU/145134.htm

### См. также:

Сценарий:Управление программами .....556

## Создание инсталляционного пакета для программы стороннего производителя из базы "Лаборатории Касперского"

Kaspersky Security Center Web Console позволяет выполнять удаленную установку программ сторонних производителей с помощью инсталляционных пакетов (см. стр. 819). Такие программы сторонних производителей включены в соответствующую базу данных "Лаборатории Касперского". База данных создается автоматически при первом запуске задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 1244).

► *Чтобы создать инсталляционный пакет для программы стороннего производителя из базы "Лаборатории Касперского":*

1. В главном меню программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. Нажмите на кнопку **Добавить**.
3. На открывшейся странице мастера создания пакета выберите параметр **Выбрать программу из базы "Лаборатории Касперского" для создания инсталляционного пакета** и нажмите на кнопку **Далее**.
4. В открывшемся списке программ выберите соответствующую программу и нажмите на кнопку **Далее**.
5. Выберите нужный язык локализации в раскрывающемся списке и нажмите на кнопку **Далее**.

   Этот шаг отображается только если программа предоставляет несколько языков.

6. Если вам будет предложено принять Лицензионное соглашение для установки, на открывшейся странице **Лицензионное соглашение** перейдите по ссылке на веб-сайте производителя, чтобы

прочитать Лицензионное соглашение, а затем установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения**.

7. На открывшейся странице **Имя нового инсталляционного пакета** в поле **Имя пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

Дождитесь загрузки созданного инсталляционного пакета на Сервер администрирования. После того как мастер создания инсталляционного пакета отобразит сообщение, информирующее вас, что процесс создания пакета успешно завершен, нажмите на кнопку **Готово**.

Созданный инсталляционный пакет появится в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка программы*.

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Просмотр и изменение параметров инсталляционного пакета для программы стороннего производителя из базы "Лаборатории Касперского"

Если вы ранее создавали какие-либо инсталляционные пакеты программ сторонних производителей, перечисленные в базе "Лаборатории Касперского" (см. стр. 1353), вы можете просмотреть и изменить параметры (см. стр. 1355) этих пакетов.

Изменение параметров инсталляционного пакета программы стороннего производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование.

Чтобы просмотреть и изменить параметры инсталляционного пакета для программы стороннего производителя из базы "Лаборатории Касперского":

1. В главном меню программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.
3. На открывшейся странице свойств измените параметры, если это требуется.
4. Нажмите на кнопку **Сохранить**.

Изменения сохранены.

### См. также:

Сценарий: Настройка защиты сети ..... 400

kaspersky

# Параметры инсталляционного пакета для программы стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета программы стороннего производителя сгруппированы на следующих закладках:

> По умолчанию отображается только часть параметров, перечисленных ниже. Вы можете добавить соответствующие графы, нажав на кнопку **Фильтр** и выбрав соответствующие графы из списка.

- Закладка **Общие**:
  - Поле ввода, содержащее название инсталляционного пакета, которое можно изменить вручную.
  - **Программа**
  - **Версия**
  - **Размер**
  - **Создан**
  - **Путь**
- Закладка **Последовательность установки**:
  - **Устанавливать требуемые общесистемные компоненты**
  - Таблица, в которой отображаются свойства обновления и которая содержит следующие графы:
    - **Имя**
    - **Описание**
    - **Источник**
    - **Тип**
    - **Категория**
    - **Уровень важности по MSRC**
    - **Уровень важности**
    - **Уровень важности патча (для патчей программ "Лаборатории Касперского")**
    - **Статья**
    - **Бюллетень**
    - **Не назначено к установке (новая версия)**
    - **Назначено к установке**
    - **Устанавливается**
    - **Установлено**
    - **Сбой**
    - **Требуется перезагрузка**
    - **Зарегистрировано**

- **Устанавливается интерактивно**
- **Отозвано**
- **Статус одобрения обновления**
- **Ревизия**
- **Идентификатор обновления**
- **Версия программы**
- **Заменяемое**
- **Заменяющее**
- **Требуется принять условия Лицензионного соглашения**
- **Поставщик**
- **Семейство программ**
- **Программа**
- **Язык локализации**
- **Не назначено к установке (новая версия)**
- **Требует установки пререквизитов**
- **Режим загрузки**
- **Является патчем**
- **Не установлено**

- Закладка **Параметры**, на которой отображаются параметры инсталляционного пакета, их названия, описания и значения, которые используются в качестве параметров командной строки во время установки. Если в пакете таких нет параметров, отображается соответствующее сообщение. Вы можете изменить значения этих параметров.
- Закладка **История ревизий**, на которой отображается версии инсталляционного пакета и которая содержит следующие графы:
  - **Ревизия**
  - **Время**
  - **Пользователь**
  - **Действие**
  - **Описание**

### См. также:

Сценарий: Настройка защиты сети ..... 400

## Теги программ

В этом разделе описаны теги программ, приведены инструкции по их созданию и изменению, а также по назначению тегов сторонним программам.

kaspersky

## См. также:



## В этом разделе



## О тегах программ

Kaspersky Security Center позволяет назначать теги сторонним программам (программам, выпущенным производителями, отличными от "Лаборатории Касперского"). Тег представляет собой метку программы, которую можно использовать для группировки и поиска программ. Назначенный программе тег можно использовать в условиях для выборок устройств (см. стр. 1146).

Например, можно создать тег `[Браузеры]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

## См. также:



## Создание тегов программ

► *Чтобы создать тег программы:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Теги программ**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов программы.

## См. также:

## Изменение тегов программ

► *Чтобы переименовать тег программы:*

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Теги программ**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените имя тега.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов программ.

### См. также:

Сценарий:Управление программами ..... 556

Сценарий: Обнаружение устройств в сети ..... 1054

## Назначение тегов программам

► *Чтобы назначить программе теги:*

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Реестр программ**.
2. Выберите программу, для которой требуется назначить теги.
3. Выберите закладку **Теги**.

   На закладке появятся все теги программ, существующие на Сервере администрирования. Теги, назначенные выбранной программе, отмечены флажками в графе **Тег назначен**.
4. Установите флажки в графе **Тег назначен** для тегов, которые требуется назначить.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены программе.

### См. также:

Сценарий:Управление программами ..... 556

Сценарий: Обнаружение устройств в сети ..... 1054

## Снятие назначенных тегов с программ

► *Чтобы снять теги с программы:*

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Реестр программ**.
2. Выберите программу, с которой требуется снять теги.
3. Выберите закладку **Теги**.

На закладке появятся все теги программ, существующие на Сервере администрирования. Теги, назначенные выбранной программе, отмечены флажками в графе **Тег назначен**.

4. Снимите флажки в графе **Тег назначен** для тегов, которые требуется снять.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с программы.

> Снятые с программ теги не удаляются. При необходимости их можно удалить вручную (см. стр. 1359).

### См. также:


Сценарий:Управление программами ..... 556

Сценарий: Обнаружение устройств в сети ..... 1054


## Удаление тегов программ

► *Чтобы удалить тег программы:*

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Теги программ**.
2. В списке выберите теги программы, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Выбранный тег программы удален. Удаленный тег автоматически снимается со всех программ, которым он был назначен.

### См. также:


Сценарий:Управление программами ..... 556

Сценарий: Обнаружение устройств в сети ..... 1054

kaspersky

# Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center можно настраивать функции мониторинга и параметры отчетов.

## В этом разделе



# Сценарий: Мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center.

**Предварительные требования**

После развертывания Kaspersky Security Center в сети организации вы можете приступить к мониторингу состояния безопасности сети с помощью Kaspersky Security Center и к формированию отчетов.

Мониторинг и работа с отчетами в сети организации состоят из следующих этапов:

**a.** Настройка переключения статусов устройств

Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры (см. стр. 1449), вы можете изменить количество событий с уровнями важности *Критический* или *Предупреждение*. При настройке переключения состояний устройства убедитесь, что:

новые параметры не противоречат политикам информационной безопасности вашей организации;

вы можете своевременно реагировать на важные события безопасности в сети вашей организации.

**b.** Настройка параметров уведомлений о событиях на клиентских устройствах

Инструкции:

Настройка уведомлений (по электронной почте, по SMS или с помощью запуска исполняемого файла) о событиях на клиентских устройствах (см. стр. 1450).

**c.** Изменение ответа вашей сети безопасности на событие Вирусная атака

Вы можете изменить пороговые значения в свойствах Сервера администрирования (см. стр. 687). Вы также можете создать более строгую политику (см. стр. 1181), которая будет активирована, или создать задачу (см. стр. 1111), которая будет запускаться при возникновении этого события.

**d.** Выполнение рекомендуемых действий для критических и предупреждающих уведомлений

Инструкции:

Выполните рекомендуемые действия для сети вашей организации (см. стр. 1442).

**e.** Просмотр состояния безопасности сети вашей организации

Инструкции:

Просмотр веб-виджета Состояние защиты (см. стр. 1363).

Генерация и просмотр отчета Отчет о состоянии защиты (см. стр. 1372).

Генерация и просмотр отчета об ошибках (см. стр. 1372).

**f.** Нахождение незащищенных клиентских устройств

Инструкции:

Просмотр веб-виджета Новые устройства (см. стр. 1363)

Генерация и просмотр отчета Отчет о состоянии защиты (см. стр. 1372).

**g.** Проверка защиты клиентских устройств

Инструкции:

Генерация и просмотр отчета из категорий Статус защиты и Статистика угроз (см. стр. 1372).

Запуск и просмотр выборки событий Критические (см. стр. 1378).

**h.** Оценка и ограничение загрузки событий в базу данных

Информация о событиях, которые возникают во время работы управляемых программ, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

Инструкции:

Расчет места в базе данных

Ограничение максимального количества событий (см. стр. 983).

**i.** Просмотр информации о лицензии

Инструкции:

Добавление веб-виджета Используемые лицензионные ключи на панель мониторинга и его просмотр (см. стр. 1363).

Генерация и просмотр отчета Отчет об использовании лицензионных ключей (см. стр. 1372).

**Результаты**

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

## См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....449

kaspersky

# О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. Kaspersky Security Center 14.2 Web Console предоставляет следующие виды мониторинга и отчетов, основанные на событиях в сети вашей организации:

- Панель мониторинга
- Отчеты
- Выборки событий
- Уведомления

**Панель мониторинга**

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

**Отчеты**

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

**Выборки событий**

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Сбой**, **Предупреждение** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 14.2 Web Console.

**Уведомления**

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

# Панель управления и веб-виджеты

В этом разделе содержится информация о панели мониторинга и веб-виджетах, представленных на панели мониторинга. Раздел содержит инструкции по управлению веб-виджетами и настройке веб-виджетов.

kaspersky

## В этом разделе



## Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Kaspersky Security Center 14.2 Web Console на закладке **Мониторинг и отчеты\Панель мониторинга**.

На панели мониторинга представлены настраиваемые веб-виджеты. Вы можете выбрать большое количество различных веб-виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в веб-виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа веб-виджета. Вы можете обновить данные веб-виджета вручную с помощью меню, в любое время.

По умолчанию веб-виджеты включают информацию о событиях, хранящихся в базе данных Сервера администрирования.

Kaspersky Security Center 14.2 Web Console имеет по умолчанию набор веб-виджетов для следующих категорий:

- **Состояние защиты.**
- **Развертывание.**
- **Обновление.**
- **Статистика угроз.**
- **Другие.**

Некоторые веб-виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

При настройке панели мониторинга можно добавлять необходимые веб-виджеты (см. стр. 1364), скрывать веб-виджеты (см. стр. 1364), а также менять внешний вид или размер веб-виджетов (см. стр. 1365), перемещать веб-виджеты(см. стр. 1364) и изменять параметры веб-виджетов (см. стр. 1365).

## См. также:

## Добавление веб-виджета на информационную панель

► *Чтобы добавить веб-виджет на информационную панель:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на кнопку **Добавить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет, который требуется добавить на информационную панель.

   Веб-виджеты сгруппированы по категориям. Чтобы посмотреть, какие веб-виджеты входят в категорию, нажмите на значок шеврона (>) рядом с именем категории.
4. Нажмите на кнопку **Добавить**.

Выбранные веб-виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид (см. стр. 1365) и параметры (см. стр. 1365) добавленных веб-виджетов.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Удаление веб-виджета с информационной панели

► *Чтобы удалить веб-виджет с информационной панели:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется удалить.
3. Выберите **Скрыть веб-виджет**.
4. В появившемся окне **Предупреждение** нажмите на кнопку **ОК**

Выбранный веб-виджет будет удален с информационной панели. В дальнейшем можно опять добавить веб-виджет на информационную панель (см. стр. 1364).

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Перемещение веб-виджета на информационной панели

► *Чтобы переместить веб-виджет на информационной панели:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется переместить.
3. Выберите **Переместить**.
4. Укажите место, куда требуется переместить веб-виджет. Можно выбрать только другой веб-виджет.

Выбранные веб-виджеты поменяются местами.

## См. также:

Сценарий: Мониторинг и отчеты .....1360

## Изменение размера или внешнего вида виджета

Можно изменить внешний вид веб-виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых веб-виджетов можно изменить размер: маленький, средний или крупный.

► *Чтобы изменить внешний вид веб-виджета:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.
3. Выполните одно из следующих действий:
   - Чтобы веб-виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы веб-виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой веб-виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

Внешний вид выбранного веб-виджета будет изменен.

## См. также:

Сценарий: Мониторинг и отчеты .....1360

## Изменение параметров веб-виджета

► *Чтобы изменить параметры веб-виджета:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.
3. Выберите **Показать параметры**.
4. В открывшемся окне параметров веб-виджета измените требуемые параметры веб-виджета.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного веб-виджета будут изменены.

Набор параметров зависит от конкретного веб-виджета. Ниже приведены некоторые общие параметры:

- **Область веб-виджета** – набор объектов, для которых веб-виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выбор задачи** – задача, для которой веб-виджет отображает информацию.
- **Период** – период, за который отображается информация в веб-виджете; например, между двумя заданными датами, от заданной даты до настоящего времени или за указанное количество дней до настоящего времени.
- **Установить статус "Критический"** и **Установить статус "Предупреждение"** – правила, в соответствии с которыми назначаются цвета на графике статусов.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга (см. стр. 1366) для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Kaspersky Security Center (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором веб-виджетов. Таким образом, пользователь может просматривать указанную в веб-виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с веб-виджетами, например, добавлять или скрывать их. Поэтому нужно разместить на панели мониторинга все необходимые пользователю веб-виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** (см. стр. 1191) в функциональной области **Общие характеристики: Права пользователей**.

### См. также:

Настройка режима Просмотра только панели мониторинга.....1366

## Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга (см. стр. 1366) убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменения списков управления доступом к объектам** (см. стр. 1191) в функциональной области **Общие функции: Права пользователей**. Если у вас нет этого права, закладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** (см. стр. 1191) в области Общий функционал: функциональная область **Базовая функциональность**.

Если в вашей сети выстроена иерархия Серверов администрирования, для настройки режима Просмотра только панели мониторинга перейдите на тот Сервер, на котором учетная запись пользователя доступна в разделе **Пользователи и роли** → **Пользователи**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга нельзя.

► *Чтобы настроить режим Просмотра только панели мониторинга:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с веб-виджетами.
3. В открывшемся окне свойств учетной записи выберите закладку **Панель мониторинга**.

   На открывшейся закладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также нельзя изменить панель мониторинга. После выключения параметра можно управлять веб-виджетами.
5. Настройте внешний вид панели мониторинга. Набор веб-виджетов, подготовленный на закладке **Панель мониторинга**, доступен для пользователя с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер веб-виджетов, добавлять или удалять веб-виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог просматривать статистику защиты сети. С этой целью на закладке **Панель мониторинга** можно выполнять те же действия с веб-виджетами, что и в разделе **Мониторинг и отчеты** → **Панель мониторинга**:
   - Добавлять веб-виджеты (см. стр. 1364) на панель мониторинга.
   - Скрывать веб-виджеты (см. стр. 1364), которые не нужны пользователю.
   - Перемещать веб-виджеты (см. стр. 1364) в определенном порядке.
   - Изменять размер или внешний вид (см. стр. 1365) веб-виджетов.
   - Изменение параметров веб-виджетов (см. стр. 1365).
6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Kaspersky Security Center, в том числе изменять параметры безопасности и веб-виджеты.
7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.
8. Если пользователь хочет просмотреть статистику поддерживаемых программ "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права (см. стр. 1191) для этого

пользователя. После этого данные программ "Лаборатории Касперского" отображаются у пользователя в веб-виджетах этих программ.

Теперь пользователь может входить в Kaspersky Security Center под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

# Отчеты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

## В этом разделе



## Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Kaspersky Security Center 14.2 Web Console на закладке **Мониторинг и отчеты\Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky Security Center имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты.**
- **Развертывание.**
- **Обновление.**
- **Статистика угроз.**
- **Другие.**

Вы можете создавать пользовательские шаблоны отчетов (см. стр. 1369), редактировать шаблоны отчетов (см. стр. 1369) и удалять их (см. стр. 1374).

Можно создавать отчеты (см. стр. 1372) на основе существующих шаблонов, экспортировать отчеты в файл (см. стр. 1372) и создавать задачи рассылки отчетов (см. стр. 1373).

## См. также:


Сценарий:Установка и первоначальная настройка Kaspersky Security Center 14.2 Web Console ....948

Сценарий: Мониторинг и отчеты ..... 1360

## Создание шаблона отчета

► *Чтобы создать шаблон отчета:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. На первой странице мастера укажите название отчета и выберите тип отчета.
4. На странице **Область действия** выберите набор клиентских устройств (групп администрирования, выборок устройств или всех сетевых устройств), данные о которых будут отображаться в отчетах, сформированных на основе этого шаблона.
5. На странице **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:
   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.
6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:
   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.
   - Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

     Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Просмотр и изменение свойств шаблона отчета

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

► *Чтобы просмотреть и изменить свойства шаблона отчета:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.

   В качестве альтернативы можно сначала сформировать отчет (см. стр. 1372), а затем нажать на кнопку **Изменить**.
3. Нажмите на кнопку **Открыть свойства шаблона отчета**.

Откроется окно **Изменение отчета <имя отчета>** на закладке **Общие**.

4. Измените свойства шаблона отчета:
   - Закладка **Общие**
     - Название шаблона отчета
     - **Максимальное число отображаемых записей**

       Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

       Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Поля отчета** → **Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

       Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

       По умолчанию параметр включен. По умолчанию указано значение 1000.

     - **Группа**

       Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

     - **Период**

       Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

       - между двумя указанными датами;
       - от указанной даты до даты создания отчета;
       - от даты создания отчета минус указанное количество дней до даты создания отчета.

     - **Включать данные подчиненных и виртуальных Серверов администрирования**

       Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

       Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

       По умолчанию параметр включен.

     - **До уровня вложенности**

       Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию подчиненных Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этой опции позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Закладка **Графы**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

## Экспорт отчета в файл

Вы можете экспортировать отчет в файл формата XML, HTML или PDF.

► *Чтобы экспортировать отчет в файл:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Установите флажок рядом с названием отчета, который требуется экспортировать в файл.
3. Нажмите на кнопку **Экспортировать отчет**.
4. В открывшемся окне измените имя файла отчета в поле **Имя**. По умолчанию имя файла совпадает с именем выбранного шаблона отчета.
5. Выберите тип файла отчета: XML, HTML или PDF.
6. Нажмите на кнопку **Экспортировать отчет**.

   Отчет будет загружен, в выбранном формате, в папку по умолчанию, на ваше устройство, или откроется стандартное окно **Сохранить как** в вашем браузере, чтобы вы могли сохранить файл в нужном вам месте.

Отчет будет сохранен в файл.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Генерация и просмотр отчета

► *Чтобы сформировать и просмотреть отчет:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В отчете отображаются следующие данные:

- На закладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета;
- На закладке **Подробнее** отобразится таблица с подробными данными отчета.

## См. также:

Сценарий:Обновление программ сторонних производителей ..... 489

Сценарий: Мониторинг и отчеты ..... 1360

## Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

► *Чтобы создать задачу рассылки отчета:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. [Не обязательно] Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Новая задача рассылки отчетов**.
4. Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На первой странице мастера укажите название задачи. По умолчанию используется название **Рассылка отчета (<N>)**, где <N> – это порядковый номер задачи.
6. На странице параметров задачи в мастере укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей. Если вы их выбрали на шаге 2, пропустите этот шаг.
   b. Формат отчета: HTML, XLS или PDF.
   c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.
   d. Будут ли отчеты сохраняться в папку, будут ли перезаписываться сохраненные ранее отчеты в этой папке и будет ли использоваться отдельная учетная запись для доступа к папке (для папки общего доступа).
7. Если требуется изменить другие параметры задачи после ее создания, на странице **Завершение создания задачи** в мастере включите параметр **Открыть окно свойств задачи после ее создания**.
8. Нажмите на кнопку **Создать**, чтобы создать задачу и закрыть мастер.

   Будет создана задача отправки отчета. Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи.

kaspersky

### См. также:



### Удаление шаблонов отчетов

► *Чтобы удалить шаблоны отчетов:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

### См. также:



## События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky Security Center, и об управлении блокировкой частых событий.

### В этом разделе



### О событиях Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

### Типы событий

В Kaspersky Security Center существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых программах "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых программ "Лаборатории Касперского". Каждая управляемая программа "Лаборатории Касперского" имеет собственный набор событий.

### События источников

События могут генерироваться следующими программами:

- Компоненты программы Kaspersky Security Center:
  - Сервер администрирования (см. стр. 619)
  - Агент администрирования (см. стр. 644)
  - Сервер iOS MDM
  - Сервер мобильных устройств Exchange ActiveSync
- Управляемые программы "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми программами "Лаборатории Касперского", см. в документации соответствующей программы.

Просмотреть полный список событий, которые может генерировать программа, можно на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

### Уровень важности событий

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

kaspersky

## Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Сбой**, **Предупреждение** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 14.2 Web Console.

Выборки событий доступны в Kaspersky Security Center 14.2 Web Console на закладке **Мониторинг и отчеты\Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky Security Center имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные сообщения.**
- **Запросы пользователей** (события управляемых программ).
- **Последние события** (за последнюю неделю).
- **События аудита** (см. стр. 1427).

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий (см. стр. 1377). В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию программы и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky Security Center отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

Вы можете выполнить следующее:

- Измените параметры выборки событий (см. стр. 1377).
- Сгенерируйте выборку событий (см. стр. 1378).
- Просмотрите сведения о выбранных выборках событий (см. стр. 1379).
- Удалите выборку событий (см. стр. 1378).
- Удалять события из базы данных Сервера администрирования (см. стр. 1393).

kaspersky

## См. также:



## В этом разделе



## Создание выборки событий

► *Чтобы создать выборку событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры выборки событий. Параметры можно указать в нескольких разделах этого окна.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

   Откроется окно подтверждения.
5. Чтобы просмотреть результат выборки событий, установите флажок **Перейти к результатам выборки**.
6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результатам выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

## См. также:



## Изменение выборки событий

► *Чтобы изменить выборку событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.
4. Отредактируйте свойства выборки событий.

> Для стандартной выборки событий можно редактировать свойства только на следующих закладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

Для пользовательских выборок можно редактировать все свойства.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Просмотр списка выборки событий

► *Просмотр выборки событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:
   - Чтобы настроить сортировку для результатов выборки событий:
     a. Нажмите на кнопку **Изменить сортировку и запустить**.
     b. В появившемся окне **Изменить сортировку для выборки событий** укажите параметры сортировки.
     c. Нажмите на имя выборки.
   - В противном случае, если вы хотите просмотреть список событий так, как они хранятся на Сервере администрирования, нажмите на название выборки.

Отобразится результат выборки событий.

### См. также:

Сценарий: Мониторинг и отчеты .....1360

## Удаление выборок событий

> Можно удалять только пользовательские выборки событий. Предопределенные выборки событий нельзя удалить.

► *Чтобы удалить выборки событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Выборка событий будет удалена.

См. также:

Сценарий: Мониторинг и отчеты .....1360

## Просмотр информации о событии

► *Чтобы просмотреть детальную информацию о событии:*

1. Запустите выборку событий (см. стр. 1378).
2. Нажмите на требуемое событие.

   Откроется окно **Свойства события**.
3. В открывшемся окне можно выполнить следующие действия:
   - Просмотреть информацию выбранного события.
   - Перейти к следующему или к предыдущему событию в списке – результате выборки событий.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

См. также:

Сценарий: Мониторинг и отчеты .....1360

## Экспорт событий в файл

► *Чтобы экспортировать события в файл:*

1. Запустите выборку событий (см. стр. 1378).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **Экспортировать в файл**.

Выбранные события экспортированы в файл.

См. также:

Сценарий: Мониторинг и отчеты .....1360

## Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

kaspersky

## В этом разделе



## Сценарий: Настройка экспорта событий в SIEM-системы

Kaspersky Security Center позволяет выполнять настройку одним из способов: экспорт в любую SIEM-систему, использующую формат Syslog, экспорт в QRadar, Splunk, ArcSight SIEM-системы, использующие форматы LEEF и CEF, или экспорт событий в SIEM-системы прямо из базы Kaspersky Security Center. По завершении этого сценария Сервер администрирования автоматически отправляет события в SIEM-систему.

**Предварительные требования**

Перед началом настройки экспорта событий в Kaspersky Security Center:

- Узнайте больше о методах экспорта событий (см. стр. 839).
- Убедитесь, что у вас есть значения системных параметров (см. стр. 838).

Вы можете выполнять шаги этого сценария в любом порядке.

Процесс экспорта событий в SIEM-систему состоит из следующих шагов:

- Настройка SIEM-системы для получения событий из Kaspersky Security Center.

  Инструкции: Настройка экспорта событий в SIEM-системе (см. стр. 841)
- Выбор события, которые вы хотите экспортировать в SIEM-систему:

  Инструкции:

  Консоль администрирования: Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog (см. стр. 843), Выбор общих событий для экспорта в формате Syslog (см. стр. 845).

  Kaspersky Security Center 14.2 Web Console: Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog (см. стр. 1385), Выбор общих событий для экспорта в формате Syslog (см. стр. 1386).
- Настройка экспорта событий в SIEM-систему одним из следующих способов:

  Укажите протоколы TCP/IP, UDP или TLS over TCP.

Инструкции:

Консоль администрирования: Настройка экспорта событий в SIEM-системы (см. стр. 847).

Kaspersky Security Center 14.2 Web Console: Настройка экспорта событий в SIEM-системы (см. стр. 1388).

Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

**Результаты**

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта (см. стр. 851), если вы выбрали события, которые хотите экспортировать.

## См. также:



## Предварительные условия

При настройке автоматического экспорта событий в Kaspersky Security Center необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center.

Для настройки автоматического экспорта событий в SIEM-систему необходимо знать значения следующих параметров:

- **Адрес сервера SIEM-системы**

  Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

- **Порт сервера SIEM-системы**

  Номер порта, по которому будет установлено соединение между Kaspersky Security Center и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

  **Протокол**Протокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

## См. также:

kaspersky

## Об экспорте событий

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center, а затем получение событий в SIEM-системе, либо наоборот.

**Способы отправки событий из Kaspersky Security Center**

Существует три способа отправки событий из Kaspersky Security Center во внешние системы:

- Отправка событий по протоколу Syslog в любую SIEM-систему.

  По протоколу Syslog можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в программах "Лаборатории Касперского", установленных на управляемых устройствах. Протокол Syslog – это стандартный протокол регистрации сообщений. Вы можете использовать этот протокол для экспорта событий в любую SIEM-систему.

  Для этого нужно отметить события, которые вы хотите передать в SIEM-систему. Вы можете отметить события с помощью Консоли администрирования (см. стр. 843) или Kaspersky Security Center 14.2 Web Console (см. стр. 1386). Только отмеченные события будут передаваться в SIEM-систему. Если вы ничего не отметили, никакие события не будут передаваться.

- Отправка событий по протоколам CEF и LEEF в системы QRadar, Splunk и ArcSight.

  Протоколы CEF и LEEF можно использовать для экспорта общих событий (на стр. 838). При экспорте событий по протоколам CEF и LEEF у вас нет возможности выбора определенных экспортируемых событий. Вместо этого выполняется экспорт всех общих событий. В отличие от протокола Syslog, протоколы CEF и LEEF не являются универсальными. Протоколы CEF и LEEF предназначены для соответствующих SIEM-систем (QRadar, Splunk и ArcSight). Поэтому при выборе экспорта событий по одному из этих протоколов в SIEM-системе используется нужный анализатор.

  > Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного лицензионного ключа (на стр. 389).

- Напрямую из базы данных Kaspersky Security Center в любую SIEM-систему.

  Этот способ экспорта событий можно использовать для получения событий напрямую из публичных представлений базы данных с помощью SQL-запросов. Результаты выполнения запроса сохраняются

в .xml файл, который можно использовать в качестве входных данных для внешней системы. Напрямую из базы данных можно экспортировать только события, доступные в публичных представлениях.

**Получение событий SIEM-системой**

SIEM-система должна принимать и корректно анализировать события, получаемые из Kaspersky Security Center. Для этого необходимо выполнить настройку SIEM-системы. Конфигурация зависит от конкретной используемой SIEM-системы. Однако в конфигурациях всех SIEM-систем существует ряд общих этапов, таких как настройка приемника и анализатора.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы.....836

## О настройке экспорта событий в SIEM-системе

В процедуре экспорта событий из Kaspersky Security Center во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center.

Настройки, выполняемые в SIEM-системе, зависят от того, какую систему вы используете. В общем случае для всех SIEM-систем необходимо настроить приемник сообщений и, при необходимости, анализатор сообщений, для того чтобы разложить полученные сообщения на поля.

**Настройка приемника сообщений**

Для SIEM-системы необходимо настроить приемник для получения событий, отправляемых Kaspersky Security Center. В общем случае в SIEM-системе необходимо указать следующие параметры:

- **Протокол экспорта или тип входных данных**

  Протокол передачи сообщений, TCP/IP или UDP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

  Номер порта для подключения к Kaspersky Security Center. Необходимо указать тот же номер порта, который был выбран в Kaspersky Security Center для передачи событий.

- **Протокол передачи сообщений или тип исходных данных**

  Протокол, используемый для экспорта событий в SIEM-систему. Это может являться одним из стандартных протоколов: Syslog, CEF или LEEF. SIEM-система выбирает анализатор событий, соответствующий указанному протоколу.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.

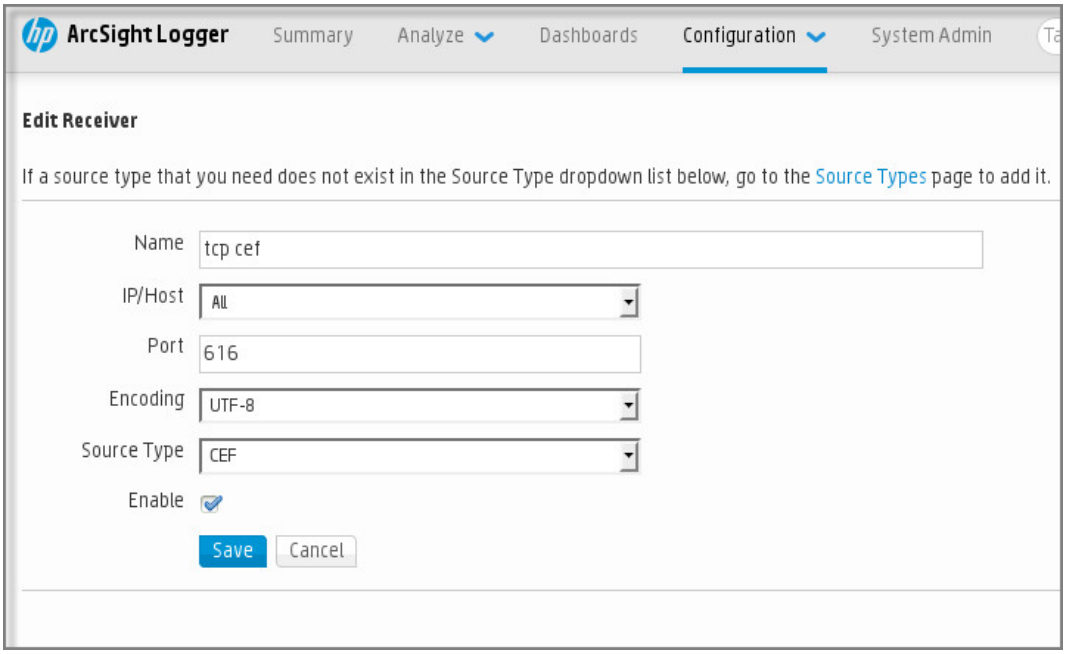



Figure 16. Пример настройки приемника сообщений

**Анализатор сообщений**

Экспортируемые события передаются в SIEM-систему в виде сообщений. Затем к этим сообщениям применяется анализатор, для того чтобы информация о событиях была должным образом передана в SIEM-систему. Анализатор сообщений встроен в SIEM-систему; он используется для разбиения сообщения на поля, такие как идентификатор сообщения, уровень важности, описание и прочие параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

В каждой SIEM-системе имеется набор стандартных анализаторов сообщений. "Лаборатория Касперского" также предоставляет анализаторы сообщений для некоторых SIEM-систем, например, для QRadar и ArcSight. Вы можете загрузить эти анализаторы сообщений с веб-страниц соответствующих SIEM-систем. При настройке приемника можно выбрать используемый анализатор сообщений: один из стандартных анализаторов вашей SIEM-системы или анализатор, предоставляемый "Лабораторией Касперского".

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы.....836

## Выбор событий для экспорта в SIEM-системы в формате Syslog

В этом разделе описывается, как выбрать события для дальнейшего экспорта в SIEM-системы в формате Syslog.

kaspersky

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## В этом разделе



### *О выборе событий для экспорта в SIEM-систему в формате Syslog*

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.
- Выбор событий для управляемой программы. Если вы выбираете экспортируемые события для управляемой программы, установленной на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

### *Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog*

Если вы хотите выполнить экспорт событий, произошедших в определенной управляемой программе, установленной на управляемых устройствах, выберите для программы события для экспорта. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

► *Чтобы отметить события для экспорта для определенной управляемой программы:*

1. В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику программы, для которой нужно отметить события.

   Откроется окно свойств политики.
3. Перейдите в раздел **Настройка событий**.
4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

> Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в графе **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.
7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемой программы готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике программы, вам не удастся переопределить выбранные события для управляемого устройства.

► *Чтобы выбрать события для управляемого устройства:*

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.
2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.
3. Перейдите в раздел **Программы**.
4. Перейдите по ссылке с названием требуемой программы в списке программ.
5. Перейдите в раздел **Настройка событий**.
6. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
7. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.
8. Флажок (✓) появляется в графе **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

## См. также:

О событиях в Kaspersky Security Center .....838

### *Выбор общих событий для экспорта в формате Syslog*

Вы можете отметить общие события, которые Сервер администрирования будет экспортировать в SIEM-системы, используя формат Syslog.

► *Чтобы выбрать общие события для экспорта в SIEM-систему:*

1. Выполните одно из следующих действий:
   - В главном меню нажмите на значок параметров (  ) рядом с именем требуемого Сервера администрирования.
   - В главном окне программы перейдите в раздел **Устройства** → **Политики и профили политик**, а затем перейдите по ссылке политики.

2. В открывшемся окне перейдите на закладку **Настройка событий**.
3. Нажмите на **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

   Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

4. Флажок (✓) появляется в графе **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.

Теперь Сервер администрирования отправляет в SIEM-систему выбранные события, если экспорт в SIEM-систему настроен.

### См. также:

О событиях в Kaspersky Security Center .....838

## Об экспорте событий в форматах CEF и LEEF

Форматы CEF и LEEF можно использовать для экспорта в SIEM-систему общих событий (на стр. 838), а также событий, переданных программами "Лаборатории Касперского" Серверу администрирования. Набор экспортируемых событий определен заранее, возможность выбирать экспортируемые события отсутствует.

Чтобы экспортировать события по протоколам CEF и LEEF, Интеграция с SIEM-системами должна быть активирована на Сервере администрирования с использованием действующего кода активации или активного лицензионного ключа (на стр. 389).

Формат экспорта можно выбрать в зависимости от того, какую SIEM-систему вы используете. В следующей таблице приведены SIEM-системы и соответствующие им форматы экспорта.

*Таблица 94. Форматы экспорта событий в SIEM-систему*

| SIEM-система | Формат экспорта |
|---|---|
| QRadar | LEEF |
| ArcSight | CEF |
| Splunk | CEF |

- LEEF – это специализированный формат событий для IBM Security QRadar SIEM. QRadar может получать, идентифицировать и обрабатывать события, передаваемые по протоколу LEEF. Для протокола LEEF должна использоваться кодировка UTF-8. Более подробную информацию о протоколе LEEF см. на веб-странице IBM Knowledge Center (https://www.ibm.com/support/knowledgecenter/).
- CEF – это стандарт управления типа "открытый журнал", который улучшает совместимость информации системы безопасности от разных сетевых устройств и приложений. Протокол CEF позволяет использовать общий формат журнала событий, чтобы системы управления предприятием могли легко получать и объединять данные для анализа.

При автоматическом экспорте Kaspersky Security Center отправляет общие события в SIEM-систему. Автоматический экспорт событий начинается сразу после включения. В этом разделе описана процедура включения автоматического экспорта событий.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 (https://tools.ietf.org/html/rfc5424) используется для экспорта событий из Kaspersky Security Center во внешние системы.

В Kaspersky Security Center можно настроить экспорт событий во внешние системы в формате Syslog.

Процесс экспорта состоит из двух шагов:

1. Включение автоматического экспорта событий. На этом шаге выполняется настройка Kaspersky Security Center таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center начинается сразу после включения автоматического экспорта.
2. Выбор событий, которые будут экспортироваться во внешнюю систему. На этом шаге вам нужно выбрать, какие события будут экспортироваться в SIEM-систему.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

В этой статье описывается, как настроить экспорт событий в SIEM-системы.

► *Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center 14.2 Web Console:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Интеграция**.
2. На закладке **Интеграция** выберите раздел **SIEM**.
3. Перейдите по ссылке **Параметры**.

   Откроется раздел **Параметры экспорта**.
4. Укажите параметры в разделе **Параметры экспорта**:
   - Адрес сервера SIEM-системы
   - Порт SIEM-системы
   - Протокол
   - Формат даты

Если вы выбрали формат Syslog, вы должны указать:

- Максимальный размер сообщения события (МБ)

5. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы [Включено]**.
6. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center. Можно создавать запросы непосредственно к публичным представлениям и извлекать из них данные о событиях или создавать собственные представления на базе существующих публичных представлений и обращаться к ним для получения требуемых данных.

**Публичные представления**

Для вашего удобства в базе данных Kaspersky Security Center предусмотрен набор публичных представлений. Описание публичных представлений приведено в документе klakdb.chm.

Публичное представление v_akpub_ev_event содержит набор полей, соответствующих параметрам событий в базе данных. В документе klakdb.chm также содержится информация о публичных представлениях, относящихся к другим объектам Kaspersky Security Center, например, устройствам, программам, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по созданию SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие программы для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center, например, имя инстанса и имя базы данных, приведена в соответствующем разделе (на стр. 850).

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## В этом разделе

### *Создание SQL-запроса с помощью утилиты klsql2*

В этом разделе приведены инструкции по загрузке и использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты.

► *Чтобы загрузить и использовать утилиту klsql2:*

1. Загрузите утилиту klsql2 (https://media.kaspersky.com/utilities/CorporateUtilities/klsql2.zip) с веб-сайта "Лаборатории Касперского". Не используйте версии утилиты klsql2, предназначенные для старых версий Kaspersky Security Center.
2. Скопируйте и извлеките содержимое архива klsql2.zip в любую папку на устройстве, на котором установлен Сервер администрирования Kaspersky Security Center.

   Пакет klsql2.zip содержит следующие файлы:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Откройте файл src.sql с помощью любого текстового редактора.
4. В файле src.sql введите требуемый SQL-запрос и сохраните файл.
5. На устройстве, на котором установлен Сервер администрирования Kaspersky Security Center, в командной строке введите следующую команду для запуска SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:

   ```
   klsql2 -i src.sql -u <имя пользователя> -p <пароль> -o result.xml
   ```

   где `<имя пользователя>` и `<пароль>` являются учетными данными учетной записи пользователя, имеющего доступ к базе данных.
6. При необходимости введите имя учетной записи и пароль пользователя, имеющего доступ к базе данных.
7. Откройте созданный файл result.xml и посмотрите результаты выполнения SQL-запроса.

Вы можете редактировать файл src.sql и создавать в нем любые SQL-запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить SQL-запрос и сохранить результаты в файл.

## См. также

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

### *Пример SQL-запроса, созданного с помощью утилиты klsql2*

В этом разделе приведен пример SQL-запроса, созданного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, произошедших на устройствах пользователей за последние 7 дней, и отсортировать его по времени возникновения событий, самые недавние события отображаются первыми.

**Пример:**

```
SELECT
e.nId,                                          /* идентификатор события
*/
e.tmRiseTime,                                   /* время возникновения
события */
e.strEventType,                                 /* внутреннее имя типа
события */
e.wstrEventTypeDisplayName,                     /* отображаемое имя
события */
e.wstrDescription,                              /* отображаемое описание
события */
e.wstrGroupName,                           /* имя группы устройств */
h.wstrDisplayName,                              /* отображаемое имя
устройства, на котором произошло событие */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp       /* IP-адрес
устройства, на котором произошло событие */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

### *Просмотр имени базы данных Kaspersky Security Center*

Может быть полезно знать имя базы данных, если вам нужно, например, отправить SQL-запрос и подключиться к базе данных из редактора скриптов SQL.

► *Чтобы просмотреть имя базы данных Kaspersky Security Center:*

1. В дереве консоли Kaspersky Security Center откройте контекстное меню узла **Сервер администрирования** по правой клавише мыши и выберите пункт **Свойства**.
2. В появившемся окне свойств Сервера администрирования выберите пункт **Дополнительно**, а затем **Информация об используемой базе данных**.
3. В разделе **Информация об используемой базе данных** обратите внимание на следующие свойства базы данных (см. рис. ниже):
   - **Имя экземпляра**

     Имя экземпляра используемой базы данных Kaspersky Security Center. Значение по умолчанию – *.\KAV_CS_ADMIN_KIT.*
   - **Имя базы данных**

     Имя базы данных SQL Kaspersky Security Center. По умолчанию указано значение *KAV*.

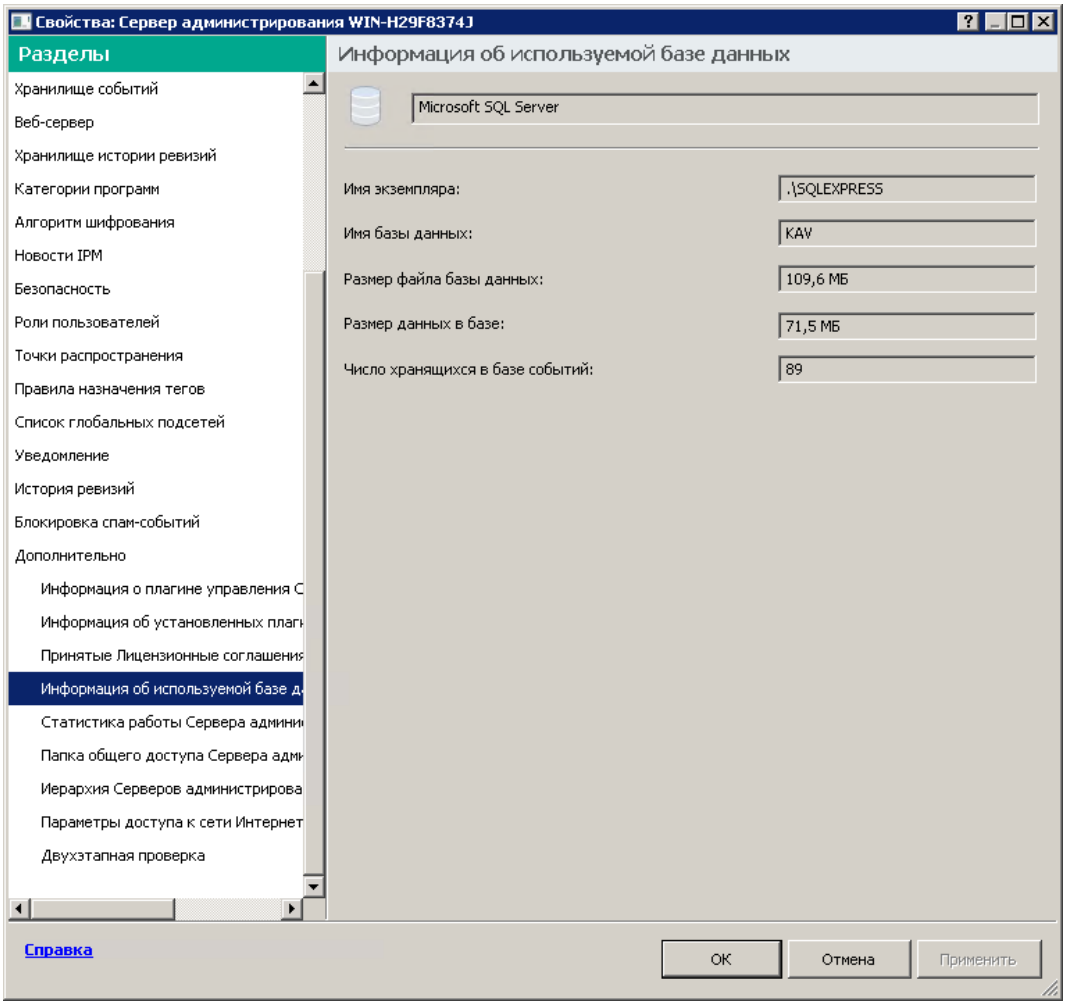



Figure 17. Имя базы данных SQL Kaspersky Security Center

4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Используйте это имя базы данных для подключения и обращения к базе данных в ваших SQL-запросах.

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Просмотр результатов экспорта

Вы можете узнать, успешно ли завершилась процедура экспорта. Для этого проверьте, были ли получены SIEM-системой сообщения, содержащие экспортируемые события.

Если отправленные из Kaspersky Security Center события получены и правильно интерпретированы SIEM-системой, значит, настройка на обеих сторонах выполнена корректно. В противном случае проверьте и при необходимости исправьте настройки Kaspersky Security Center и SIEM-системы.

Ниже приведен пример событий, экспортированных в систему ArcSight. Например, первое событие – это критическое событие Сервера администрирования: *Статус устройства "Критический"*.

Отображение экспортированных событий зависит от используемой SIEM-системы.

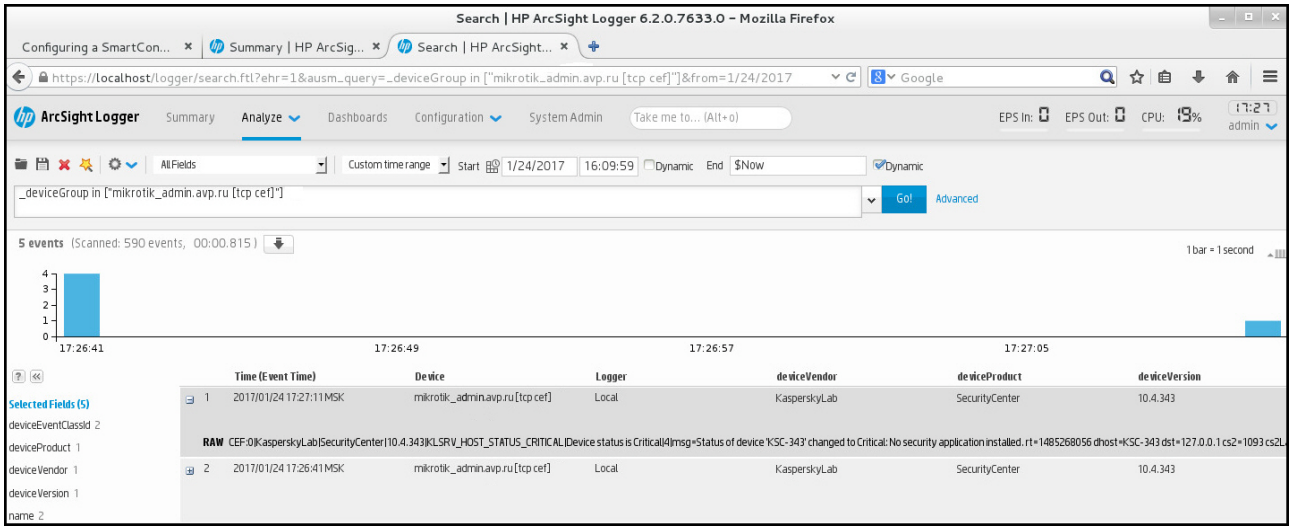



Figure 18. Пример событий

## См. также:

Сценарий: Настройка экспорта событий в SIEM-системы ..... 836

## Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями (см. стр. 811), вы можете перейти к истории ревизий объекта.

► *Чтобы просмотреть историю объекта из события:*

1. Запустите выборку событий (см. стр. 1378).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

## См. также:

Сценарий: Мониторинг и отчеты ..... 1360

## Удаление событий

► *Чтобы удалить одно или несколько событий:*

1. Запустите выборку событий (см. стр. 1378).
2. Установите флажки рядом с требуемыми событиями.
3. Нажмите на кнопку **Удалить**.

Выбранные события удалены и не могут быть восстановлены.

См. также:

Сценарий: Мониторинг и отчеты .....1360

## Настройка срока хранения события

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике программы "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного интервала времени.

► *Чтобы задать срок хранения события в базе данных Сервера администрирования:*

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Выполните одно из следующих действий:
   - Чтобы настроить срок хранения событий Агента администрирования или управляемой программы "Лаборатории Касперского" нажмите на имя соответствующей политики.

     Откроется страница свойств политики.
   - Чтобы настроить события Сервера администрирования, в главном меню нажмите на значок параметров (  ) рядом с именем требуемого Сервера администрирования.

     Если у вас есть политика для Сервера администрирования, вы можете нажать на название этой политики.

     Откроется страница свойств Сервера администрирования (или страница свойств политики Сервера администрирования).
3. Выберите закладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий.
4. Выберите раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
5. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.
6. В поле редактирования под переключателем укажите количество дней для сохранения события.
7. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

> Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования Kaspersky Security Center, вы не сможете изменить значение срока хранения события.

8. Нажмите на кнопку **ОК**.

   Окно свойств политики закроется.

Теперь, когда Сервер администрирования получает и сохраняет события выбранного типа, они будут иметь измененный срок хранения. Сервер администрирования не изменяет срок хранения ранее полученных событий.

## События компонентов Kaspersky Security Center

Каждый компонент Kaspersky Security Center имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center, Агенте администрирования, Сервере iOS MDM и Сервере мобильных устройств Exchange ActiveSync. Типы событий, которые возникают в программах "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

### В этом разделе



### Структура данных описания типа события

Для каждого типа событий отображаются его имя, идентификатор, буквенный код, описание и время хранения по умолчанию.

- **Отображаемое имя типа события**. Этот текст отображается в Kaspersky Security Center, когда вы настраиваете события и при их возникновении.
- **Идентификатор типа события**. Этот цифровой код используется при обработке событий с использованием инструментов анализа событий сторонних производителей.
- **Тип события** (буквенный код). Этот код используется при просмотре и обработке событий с использованием публичных представлений базы данных Kaspersky Security Center и при экспорте событий в SIEM-системы.
- **Описание**. Этот текст содержит описание ситуации при возникновении события и описание того, что вы можете сделать в этом случае.
- **Срок хранения по умолчанию**. Это количество дней, в течение которых событие хранится в базе данных Сервера администрирования и отображается в списке событий Сервера администрирования. После окончания этого периода событие удаляется. Если значение времени хранения события указано 0, такие события регистрируются, но не отображаются в списке событий Сервера

администрирования. Если вы настроили хранение таких событий в журнале событий операционной системы, вы можете найти их там.

Можно изменить время хранения событий:

- Консоль администрирования: Настройка срока хранения события (см. стр. 686)
- Kaspersky Security Center 14.2 Web Console: Настройка срока хранения события (см. стр. 1394)

Другие данные могут включать следующие поля:

- **event_id**: уникальный номер события в базе данных, генерируемый и присваиваемый автоматически. Его не нужно путать с **Идентификатором типа события**.
- **task_id**: идентификатор задачи, в результате выполнения которой возникло событие (если такая есть).
- **severity**: один из следующих уровней важности (в порядке возрастания важности):

  0) Недопустимый уровень важности.

  1) Информационное.

  2) Предупреждение.

  3) Ошибка.

  4) Критическое.

## События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

## В этом разделе



### *Критические события Сервера администрирования*

В таблице ниже приведены типы событий Сервера администрирования Kaspersky Security Center, объединенные по уровню важности **Критическое событие**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 95. Критические события Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Лицензионное ограничение превышено.** | 4099 | KLSRV_EV_LICENSE_CHECK_MORE_110 | Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения.<br>События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц (на стр. 343), охватываемых лицензией.<br>Даже если возникает это событие, клиентские устройства защищены.<br>Вы можете ответить на событие | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | следующими способами:<br>• Просмотрите список управляемых устройств. Удалите устройства, которые не используются.<br>• Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования).<br>Kaspersky Security Center определяет правила генерации событий (на стр. 341) при превышении лицензионного ограничения. | |
| **Вирусная атака.** | 26 (для компонента Защита от файловых угроз) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (на стр. 687).<br>• Создайте более строгую политику (на стр. 432), которая будет активирована, или создайте задачу (на стр. 413), которая будет запускаться при возникновении этого события. | |
| **Вирусная атака.** | 27 (для компонента Защита от почтовых угроз) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (на стр. 687). | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Создайте более строгую политику (на стр. 432), которая будет активирована, или создайте задачу (на стр. 413), которая будет запускаться при возникновении этого события. | |
| **Вирусная атака.** | 28 (для сетевого экрана) | GNRL_EV_VIRUS_OUTBREAK | События этого типа возникают, если количество вредоносных объектов, обнаруженных на нескольких управляемых устройствах в течение короткого периода, превышает заданные пороговые значения.<br>Вы можете ответить на событие следующими способами:<br>• Настройте пороговые значения в свойствах Сервера администрирования (см. стр. 687).<br>• Создайте более строгую политику (см. стр. 432), которая будет активирована, или создайте задачу (см. стр. 413), которая будет запускаться при | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | возникновении этого события. | |
| **Устройство стало неуправляемым.** | 4111 | KLSRV_HOST_OUT_CONTROL | События этого типа возникают, если управляемое устройство видимо в сети, но не подключено к Серверу администрирования в течение заданного периода.<br>Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства. | 180 дней |
| **Статус устройства "Критический".** | 4113 | KLSRV_HOST_STATUS_CRITICAL | События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия (на стр. 727) при выполнении которых, статус устройства изменяется на *Критический*. | 180 дней |
| **Файл ключа в списке запрещенных.** | 4124 | KLSRV_LICENSE_BLACKLISTED | События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Обратитесь в Службу технической поддержки (см. стр. 1489) для получения подробной информации. | |
| **Режим ограниченной функциональности.** | 4130 | KLSRV_EV_LICENSE_SRV_LIMITED_MODE | События этого типа возникают, если Kaspersky Security Center начинает работать в режиме базовой функциональности (см. стр. 356), без поддержки Управления мобильными устройствами и Системного администрирования.<br>Ниже приведены причины и соответствующие ответы на событие:<br>• Срок действия лицензии истек. Предоставьте лицензию на полную функциональность Kaspersky Security Center (добавьте действительный код активации или файл ключа на Сервер администрирования).<br>• Сервер администрирования управляет большим количеством устройств, чем может | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | использоваться по предоставленной лицензии. Переместите устройства из состава групп администрирования одного Сервера в группы администрирования другого Сервера (если лицензионное ограничение другого Сервера не превышено). | |
| **Срок действия лицензии истекает.** | 4129 | KLSRV_EV_LICENSE_SRV_EXPIRE_SOON | События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии (см. стр. 342).<br>Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Вы не можете изменить количество дней. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | опубликовано до следующего дня.<br>После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (см. стр. 356).<br>Вы можете ответить на событие следующими способами:<br>• Убедитесь, что резервный лицензионный ключ (см. стр. 344) добавлен на Сервер администрирования.<br>• Если вы используете подписку (см. стр. 345), продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена. | |
| **Срок действия сертификата истек.** | 4132 | KLSRV_CERTIFICATE_EXPIRED | События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для Управления | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | мобильными устройствами.<br>Вам необходимо обновить сертификат, срок действия которого истекает.<br>Вы можете настроить автоматическое обновление сертификатов, установив флажок **Автоматически перевыпускать сертификат, если это возможно** в параметрах выпуска сертификата. | |
| **Обновления модулей программ "Лаборатории Касперского" отозваны.** | 4142 | KLSRV_SEAMLESS_UPDATE_REVOKED | События этого типа возникают, если обновления (см. стр. 1259) были отозваны техническими специалистами "Лаборатории Касперского", например, по причине их замены на более новые версии. Для таких обновлений отображается статус *Отозвано*. Событие не относится к патчам Kaspersky Security Center и не относится к модулям управляемых программ "Лаборатории Касперского". Событие содержит причину, из-за которой обновления не установлены. | 180 дней |

## См. также:



### *События отказа функционирования Сервера администрирования*

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 96. События отказа функционирования Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Ошибка времени выполнения.** | 4125 | KLSRV_RUNTIME_ERROR | События этого типа возникают из-за неизвестных проблем.<br>Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением.<br>Подробную информацию о событии можно найти в его описании. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Для одной из групп лицензионных программ превышено ограничение числа установок.** | 4126 | KLSRV_INVLICPROD_EXCEDED | Сервер администрирования генерирует события такого типа периодически (каждый час). События этого типа возникают, если в Kaspersky Security Center вы управляете лицензионными ключами программ сторонних производителей и если количество установок превысило заданное в лицензионном ключе программы стороннего производителя ограничение.<br>Вы можете ответить на событие следующими способами: | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Просмотрите список управляемых устройств. Удалите программу стороннего производителя с устройств, на которых она не используется.<br>• Используйте лицензию стороннего производителя на большее количество устройств.<br>Вы можете управлять лицензионными ключами программ сторонних производителей (см. стр. 573), используя функциональность групп лицензионных программ. В группу лицензионных программ входят программы сторонних производителей, отвечающие заданным вами критериям. | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Не удалось выполнить опрос облачного сегмента.** | 4143 | KLSRV_KLCLOUD_SCAN_ERROR | События этого типа возникают, если Сервер администрирования не может опросить сегмент сети в облачном окружении. Прочтите информацию в описании события и отреагируйте соответствующим образом. | Не хранится |
| **Не удалось выполнить копирование обновлений в заданную папку.** | 4123 | KLSRV_UPD_REPL_FAIL | События этого типа возникают, если обновления программного обеспечения копируются в общую папку (или папки).<br>Вы можете ответить на событие следующими способами:<br>• Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Проверьте, не были ли изменены имя пользователя и / или пароль к папке (к папкам).<br>• Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и программных модулей (см. стр. 461). | |
| **Нет свободного места на диске.** | 4107 | KLSRV_DISK_FULL | События этого типа возникают, если на жестком диске устройства, на котором установлен Сервер администрирования, заканчивается дисковое пространство.<br>Освободите дисковое пространство на устройстве. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Недоступна папка общего доступа.** | 4108 | KLSRV_SHARED_FOLDER_UNAVAILABLE | События этого типа возникают, если общая папка Сервера администрирования (см. стр. 236) недоступна.<br>Вы можете ответить на событие следующими способами:<br>• Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен.<br>• Проверьте, были ли изменены имя пользователя и / или пароль к папке.<br>• Проверьте подключение к сети. | 180 дней |
| **Недоступна база данных Сервера администрирования.** | 4109 | KLSRV_DATABASE_UNAVAILABLE | События этого типа возникают, если база Сервера администрирования становится недоступной. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Вы можете ответить на событие следующими способами:<br>• Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер.<br>• Просмотрите журналы событий СУБД и найдите причину недоступности базы Сервера администрирования. Например, из-за профилактических работ удаленный сервер с установленным SQL Server может быть недоступен. | |
| **Нет свободного места в базе данных Сервера администрирования.** | 4110 | KLSRV_DATABASE_FULL | События этого типа возникают, если нет свободного места в базе Сервера администрирования. | 180 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна.<br>Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие:<br>• Вы используете SQL Server Express Edition: | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных. Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983). | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.<br>• Вы используете СУБД, отличную от SQL Server Express Edition:<br>Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983). | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394). Просмотрите информацию о выборе СУБД (на стр. 164). | |

## См. также:



### *События предупреждения Сервера администрирования*

В следующей таблице приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 97. События предупреждения Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Обнаружено получение частого события.** | | KLSRV_EVENT_SPAM_EVENTS_DETECTED | События этого типа возникают, если Сервер администрирования регистрирует частые события на устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий (см. стр. 651). | 90 дней |
| **Лицензионное ограничение превышено.** | 4098 | KLSRV_EV_LICENSE_CHECK_100_110 | Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения.<br>События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц (см. стр. 343) одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией.<br>Даже если возникает это событие, клиентские устройства защищены.<br>Вы можете ответить на событие следующими способами:<br>• Просмотрите список управляемых устройств. Удалите устройства, которые не используются.<br>• Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Kaspersky Security Center определяет правила генерации событий (см. стр. 341) при превышении лицензионного ограничения. | |
| **Устройство долго не проявляет активности в сети.** | 4103 | KLSRV_EVENT_HOSTS_NOT_VISIBLE | События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени.<br>Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации.<br>Вы можете ответить на событие следующими способами:<br>• Удалите устройство из списка управляемых устройств вручную.<br>• Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Консоли администрирования (см. стр. 656) или с помощью Kaspersky Security Center 14.2 Web Console (см. стр. 1131).<br>• Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Консоли администрирования (см. стр. 656) или Kaspersky Security Center 14.2 Web Console (см. стр. 1131). | 90 дней |
| **Конфликт имен устройств.** | 4102 | KLSRV_EVENT_HOSTS_CONFLICT | События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания программ на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве.<br>Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска (см. стр. 867) на эталонном устройстве. | |
| **Статус устройства "Предупреждение".** | 4114 | KLSRV_HOST_STATUS_WARNING | События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия (см. стр. 727) при выполнении которых, статус устройства изменяется на *Предупреждение*. | 90 дней |
| **Для одной из групп лицензионных программ скоро будет превышено ограничение числа установок.** | 4127 | KLSRV_INVLICPROD_FILLED | События этого типа возникают, если количество установок программ сторонних производителей, включенных в группу лицензионных программ (см. стр. 554), достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа (см. стр. 573).<br>Вы можете ответить на событие следующими способами:<br>• Если программа стороннего производителя не используется на каких-то управляемых устройствах, удалите программу с этих устройств. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Если вы ожидаете, что количество установок для программы стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии программы стороннего производителя на большее количество устройств заранее.<br>Вы можете управлять лицензионными ключами программ сторонних производителей (см. стр. 573), используя функциональность групп лицензионных программ. | |
| **Сертификат запрошен.** | 4133 | KLSRV_CERTIFICATE_REQUESTED | События этого типа возникают, если не удается автоматически перевыпустить сертификат для Управления мобильными устройствами.<br>Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие:<br>• Автоматический перевыпуск был инициирован для сертификата, для которого параметр **Автоматически перевыпускать сертификат, если это возможно** выключен. Это могло произойти из-за ошибки, которая возникла при создании сертификата. Может потребоваться перевыпуск сертификата вручную. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • Если вы используете интеграцию с инфраструктурой открытых ключей, причиной может быть отсутствие атрибута SAM-Account-Name учетной записи, которая используется для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи. | |
| **Сертификат удален.** | 4134 | KLSRV_CERTIFICATE_REMOVED | События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами.<br>После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования.<br>Это событие может быть полезно при исследовании неисправностей, связанных с Управлением мобильными устройствами. | 90 дней |
| **Срок действия APNs-сертификата истек.** | 4135 | KLSRV_APN_CERTIFICATE_EXPIRED | События этого типа происходят, если истекает срок действия APNs-сертификата.<br>Вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. | Не хранится |
| **Срок действия APNs-сертификата истекает.** | 4136 | KLSRV_APN_CERTIFICATE_EXPIRES_SOON | События этого типа возникают, если до истечения срока действия APNs-сертификата остается менее 14 дней.<br>При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. | Не хранится |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия. | |
| **Не удалось отправить GCM-сообщение на мобильное устройство.** | 4138 | KLSRV_GCM_DEVICE_ERROR | События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения к управляемым мобильным устройствам с операционной системой Android, а FCM-сервер не может обработать некоторые запросы, полученные от Сервера администрирования. Это означает, что некоторые управляемые мобильные устройства не будут получать push-уведомление.<br>Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes"). | 90 дней |
| **HTTP ошибка при отправке GCM сообщения на GCM сервер.** | 4139 | KLSRV_GCM_HTTP_ERROR | События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых мобильных устройств с операционной системой Android, а FCM-сервер возвращает запрос Серверу администрирования с кодом HTTP, отличным от 200 (OK). | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие:<br>• Проблемы на стороне FCM-сервера. Прочтите HTTP код в описании события и ответьте соответствующим образом. Дополнительная информация о HTTP кодах, полученных от FCM-сервера, и связанных с ними ошибках есть в документации службы Google Firebase https://firebase.google.com/docs/cloud-messaging/http-server-ref (см. главу "Downstream message error response codes").<br>• Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом. | |
| **Не удалось отправить GCM-сообщение на GCM сервер.** | 4140 | KLSRV_GCM_GENERAL_ERROR | События этого типа возникают из-за непредвиденных ошибок на стороне Сервера администрирования при работе с HTTP-протоколом Google Firebase Cloud Messaging.<br>Прочтите информацию в описании события и отреагируйте соответствующим образом.<br>Если вы не можете найти решение проблемы самостоятельно, рекомендуем вам обратиться в Службу технической поддержки "Лаборатории Касперского". | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Мало свободного места на диске.** | 4105 | KLSRV_NO_SPACE_ON_VOLUMES | События этого типа возникают, если на устройстве, на котором установлен Сервер администрирования, почти закончилось дисковое пространство.<br>Освободите дисковое пространство на устройстве. | 90 дней |
| **Мало свободного места в информационной базе Сервера администрирования.** | 4106 | KLSRV_NO_SPACE_IN_DATABASE | События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать.<br>Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие.<br>Вы используете SQL Server Express Edition:<br>• Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных.<br>• Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983). | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Windows, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.<br>Вы используете СУБД, отличную от SQL Server Express Edition:<br>• Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394).<br>Просмотрите информацию о выборе СУБД (см. стр. 164). | |
| **Разорвано соединение с подчиненным Сервером администрирования.** | 4116 | KLSRV_EV_SLAVE_SRV_DISCONNECTED | События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования.<br>Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом. | 90 дней |
| **Разорвано соединение с главным Сервером администрирования.** | 4118 | KLSRV_EV_MASTER_SRV_DISCONNECTED | События этого типа возникают при разрыве соединения с главным Сервером администрирования. | 90 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| | | | Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом. | |
| **Зарегистрированы новые обновления модулей программ "Лаборатории Касперского".** | 4141 | KLSRV_SEAMLESS_UPDATE_REGISTERED | События этого типа возникают, если Сервер администрирования регистрирует новые обновления программ "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение.<br>Одобрите или отклоните обновления с помощью Консоли администрирования (см. стр. 493) или Kaspersky Security Center Web Console (см. стр. 1259). | 90 дней |
| **Началось удаление событий из базы данных, так как превышено ограничение числа событий.** | 4145 | KLSRV_EVP_DB_TRUNCATING | События такого типа возникают, если удаление старых событий из базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (на стр. 686).<br>Вы можете ответить на событие следующими способами:<br>• Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 1394). | Не хранится |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Удалены события из базы данных, так как превышено ограничение числа событий.** | 4146 | KLSRV_EVP_DB_TRUNCATED | События такого типа возникают, если старые события удалены из базы данных Сервера администрирования после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования (см. стр. 686).<br>Вы можете ответить на событие следующими способами:<br>• Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования (на стр. 983).<br>• Сократите список событий для хранения в базе данных Сервера администрирования (см. стр. 1394). | Не хранится |

## См. также:



### *Информационные события Сервера администрирования*

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 98. Информационные события Сервера администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Ключ использован более чем на 90%.** | 4097 | KLSRV_EV_LICENSE_CHECK_90 | 30 дней | |
| **Найдено новое устройство.** | 4100 | KLSRV_EVENT_HOSTS_NEW_DETECTED | 30 дней | |
| **Устройство автоматически добавлено в группу.** | 4101 | KLSRV_EVENT_HOSTS_NEW_REDIRECTED | 30 дней | |
| **Устройство удалено из группы: долгое отсутствие активности в сети.** | 4104 | KLSRV_INVISIBLE_HOSTS_REMOVED | 30 дней | |
| **Для одной из групп лицензионных программ число разрешенных установок исчерпано более чем на 95%.** | 4128 | KLSRV_INVLICPROD_EXPIRED_SOON | 30 дней | |
| **Появились файлы для отправки на анализ в "Лабораторию Касперского".** | 4131 | KLSRV_APS_FILE_APPEARED | 30 дней | |
| **Регистрационный GCM-идентификатор мобильного устройства изменен.** | 4137 | KLSRV_GCM_DEVICE_REGID_CHANGED | 30 дней | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Обновления успешно скопированы в заданную папку.** | 4122 | KLSRV_UPD_REPL_OK | 30 дней | |
| **Установлено соединение с подчиненным Сервером администрирования.** | 4115 | KLSRV_EV_SLAVE_SRV_CONNECTED | 30 дней | |
| **Установлено соединение с главным Сервером администрирования.** | 4117 | KLSRV_EV_MASTER_SRV_CONNECTED | 30 дней | |
| **Базы обновлены.** | 4144 | KLSRV_UPD_BASES_UPDATED | 30 дней | |
| **Аудит: Установлено соединение с Сервером администрирования.** | 4147 | KLAUD_EV_SERVERCONNECT | 30 дней | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Аудит: Изменение объекта.** | 4148 | KLAUD_EV_OBJECTMODIFY | 30 дней | Это событие отслеживает изменения в следующих объектах:<br>• группах администрирования;<br>• группах пользователей;<br>• пользователях;<br>• инсталляционных пакетах;<br>• задачах;<br>• политиках;<br>• Серверах администрирования;<br>• виртуальных Серверах. |
| **Аудит: Изменение статуса объекта.** | 4150 | KLAUD_EV_TASK_STATE_CHANGED | 30 дней | Например, это событие возникает, если задача завершилась ошибкой. |
| **Аудит: Изменение параметров группы.** | 4149 | KLAUD_EV_ADMGROUP_CHANGED | 30 дней | |
| **Аудит: Подключение к Серверу администрирования было прервано.** | 4151 | KLAUD_EV_SERVERDISCONNECT | 30 дней | |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию | Комментарий |
|---|---|---|---|---|
| **Аудит: Свойства объекта были изменены.** | 4152 | KLAUD_EV_OBJECTPROPMODIFIED | 30 дней | Это событие отслеживает изменения в следующих параметрах:<br>• пользователь;<br>• лицензия;<br>• Серверах администрирования;<br>• виртуальный Сервер. |
| **Аудит: Права пользователя были изменены.** | 4153 | KLAUD_EV_OBJECTACLMODIFIED | 30 дней | |
| **Аудит: Импорт или экспорт ключей шифрования с Сервера администрирования.** | 5100 | KLAUD_EV_DPEKEYSEXPORT | 30 дней | |

## События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

### В этом разделе



#### *События отказа функционирования Агента администрирования*

В таблице ниже приведены типы событий Агента администрирования Kaspersky Security Center с уровнем важности **Отказ функционирования**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 99. События отказа функционирования Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Ошибка при установке исправления.** | 7702 | KLNAG_EV_PATCH_INSTALL_ERROR | События этого типа возникают, если автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center (см. стр. 476) прошла неуспешно. Событие не относится к обновлениям управляемых программ "Лаборатории Касперского".<br>Прочтите описание события. Причиной этого события может быть проблема операционной системы Windows на Сервере администрирования. Если в описании упоминается какая-либо проблема конфигурации Windows, устраните эту проблему. | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Не удалось установить обновления стороннего производителя.** | 7697 | KLNAG_EV_3P_PATCH_INSTALL_ERROR | События этого типа возникают, если используются возможности Системного администрирования и Управления мобильными устройствами (см. стр. 353), и если обновление программного обеспечения сторонних производителей (см. стр. 488) прошло неуспешно.<br>Проверьте, корректна ли ссылка на программу стороннего производителя. Прочтите описание события. | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Описание | Срок хранения по умолчанию |
|---|---|---|---|---|
| **Не удалось установить обновления Центра обновления Windows.** | 7717 | KLNAG_EV_WUA_INSTALL_ERROR | События этого типа возникают, если обновления Центра обновления Windows были неуспешными. Настройте обновления Microsoft Windows в политике Агента администрирования (см. стр. 513).<br>Прочтите описание события. Поищите описание ошибки в базе знаний Microsoft. Обратитесь в службу технической поддержки Microsoft, если вы не можете решить проблему самостоятельно. | 30 дней |

## См. также:



### *События предупреждения Агента администрирования*

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Предупреждение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 100. События предупреждения Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Установка обновления программных модулей завершена с предупреждением.** | 7701 | KLNAG_EV_PATCH_INSTALL_WARNING | 30 дней |
| **Установка обновления стороннего ПО завершена с предупреждением.** | 7696 | KLNAG_EV_3P_PATCH_INSTALL_WARNING | 30 дней |
| **Установка обновления стороннего ПО отложена.** | 7698 | KLNAG_EV_3P_PATCH_INSTALL_SLIPPED | 30 дней |
| **Произошел инцидент.** | 549 | GNRL_EV_APP_INCIDENT_OCCURED | 30 дней |
| **Прокси-сервер KSN был запущен. Не удалось проверить доступность KSN.** | 7718 | KSNPROXY_STARTED_CON_CHK_FAILED | 30 дней |

## См. также:


События отказа функционирования Агента администрирования .....645

Информационные события Агента администрирования .....648


### *Информационные события Агента администрирования*

В таблице ниже приведены события Агента администрирования Kaspersky Security Center, объединенные по уровню важности **Информационное событие**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений (на стр. 1450) в свойствах Сервера администрирования.

*Таблица 101. Информационные события Агента администрирования*

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Обновление программных модулей успешно установлено.** | 7699 | KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY | 30 дней |
| **Запущена установка обновления программных модулей.** | 7700 | KLNAG_EV_PATCH_INSTALL_STARTING | 30 дней |
| **Установлена программа.** | 7703 | KLNAG_EV_INV_APP_INSTALLED | 30 дней |
| **Программа удалена.** | 7704 | KLNAG_EV_INV_APP_UNINSTALLED | 30 дней |
| **Установлена наблюдаемая программа.** | 7705 | KLNAG_EV_INV_OBS_APP_INSTALLED | 30 дней |
| **Установлена наблюдаемая программа.** | 7706 | KLNAG_EV_INV_OBS_APP_UNINSTALLED | 30 дней |
| **Установлена сторонняя программа.** | 7707 | KLNAG_EV_INV_CMPTR_APP_INSTALLED | 30 дней |
| **Новое устройство добавлено.** | 7708 | KLNAG_EV_DEVICE_ARRIVAL | 30 дней |
| **Устройство удалено.** | 7709 | KLNAG_EV_DEVICE_REMOVE | 30 дней |
| **Обнаружено устройство.** | 7710 | KLNAG_EV_NAC_DEVICE_DISCOVERED | 30 дней |
| **Устройство авторизовано.** | 7711 | KLNAG_EV_NAC_HOST_AUTHORIZED | 30 дней |
| **Совместный доступ к рабочему столу Windows: файл был прочитан.** | 7712 | KLUSRLOG_EV_FILE_READ | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Совместный доступ к рабочему столу Windows: файл был изменен.** | 7713 | KLUSRLOG_EV_FILE_MODIFIED | 30 дней |
| **Совместный доступ к рабочему столу Windows: программа была запущена.** | 7714 | KLUSRLOG_EV_PROCESS_LAUNCHED | 30 дней |
| **Совместный доступ к рабочему столу Windows: запускается.** | 7715 | KLUSRLOG_EV_WDS_BEGIN | 30 дней |
| **Совместный доступ к рабочему столу Windows: Остановлена.** | 7716 | KLUSRLOG_EV_WDS_END | 30 дней |
| **Установка обновления стороннего ПО завершена успешно.** | 7694 | KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY | 30 дней |
| **Запущена установка обновления стороннего ПО.** | 7695 | KLNAG_EV_3P_PATCH_INSTALL_STARTING | 30 дней |

| Отображаемое имя типа события | Идентификатор типа события | Тип события | Срок хранения по умолчанию |
|---|---|---|---|
| **Прокси-сервер KSN был запущен. Проверка доступности KSN прошла успешно.** | 7719 | KSNPROXY_STARTED_CON_CHK_OK | 30 дней |
| **Прокси-сервер KSN был остановлен.** | 7720 | KSNPROXY_STOPPED | 30 дней |

### См. также:



## Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

### В этом разделе



### О блокировке частых событий

Управляемая программа, например Kaspersky Endpoint Security для Windows, установленная на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных (см. стр. 983).

Сервер администрирования автоматически блокирует получение частых событий. Вы не можете заблокировать частые события самостоятельно или выбрать, какие события заблокировать.

Чтобы узнать, заблокировано ли событие, вы можете просмотреть список уведомлений или просмотреть, присутствует ли это событие в свойствах Сервера администрирования в разделе **Блокировка частых событий**. Если событие заблокировано, можно выполнить следующие действия:

- Если вы хотите предотвратить перезапись базы данных, вы можете продолжать блокировать (на стр. 1439) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (на стр. 1439) частые события и в любом случае продолжить получение событий этого типа.
- Если вы хотите продолжать получать частые события до тех пор, пока они снова не будут заблокированы, вы можете отменить блокировку (на стр. 1440) частых событий.

## См. также:



## Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

► *Чтобы управлять блокировкой частых событий:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий**:
   - Если вы хотите разблокировать прием частых событий:
     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.
     b. Нажмите на кнопку **Сохранить**.
   - Если вы хотите заблокировать прием частых событий:
     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировать**.
     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

## См. также:

### Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

► *Чтобы отменить блокировку частых событий:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Блокировка частых событий**.
3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.
4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

### См. также:

О блокировке частых событий ..... 1438

## Получение событий от Kaspersky Security для Microsoft Exchange Servers

Информация о событиях при работе управляемых программ, таких как Kaspersky Endpoint Security для Windows, передается с управляемых устройств и регистрируется в базе данных Сервера администрирования. По умолчанию события от Kaspersky Security для Microsoft Exchange Servers не регистрируются в базе данных Сервера администрирования. Если Kaspersky Security для Microsoft Exchange Servers установлен на управляемых устройствах в вашей организации и вы хотите получать события от этой программы, включите регистрацию событий этой программы с помощью утилиты klscflag.

► *Чтобы включить регистрацию событий Kaspersky Security для Microsoft Exchange Servers:*

1. На устройстве Сервера администрирования запустите командную строку Windows под учетной записью с правами администратора.
2. Измените текущую директорию на папку установки Kaspersky Security Center (обычно это C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Выполните одну из следующих команд:
   - Для установленного Сервера администрирования на отказоустойчивом кластере Microsoft:

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```
   - Для Сервера администрирования, установленного на узле отказоустойчивого кластера "Лаборатории Касперского":

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```
   - Для Сервера администрирования, не работающего на кластере:

```
klscflag.exe -fset -pv klserver -n
KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

Регистрация событий для Kaspersky Security для Microsoft Exchange Servers включена.

Для Kaspersky Security для Microsoft Exchange Servers вы не можете задать срок хранения событий или выбрать, какие события должны сохраняться в хранилище Сервера администрирования. Вы можете установить максимальное количество событий, которые можно сохранить в хранилище (см. стр. 983). Этот параметр применяется к событиям, полученным от всех программ "Лаборатории Касперского".

# Уведомления и статусы устройств

В этом разделе содержится информация о том, как просматривать уведомления, настраивать доставку уведомлений, использовать статусы устройств и включать изменение статусов устройств.

## В этом разделе



## Использование уведомлений

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- экранные уведомления;
- уведомление по SMS;
- уведомление по электронной почте;
- уведомление запуском исполняемого файла или скрипта.

### Экранные уведомления

Экранные уведомления предупреждают вас о событиях, сгруппированных по уровням важности (*Критическое уведомление*, *Предупреждающие уведомление*, и *Информационное уведомление*).

Экранные уведомления могут иметь один из двух статусов:

- *Просмотрено*. Это означает, что вы выполнили рекомендованное действие для уведомления или вы назначили этот статус для уведомления вручную.
- *Не просмотрено*. Это означает, что вы не выполнили рекомендуемое действие для уведомления или не назначили этот статус для уведомления вручную.

По умолчанию в список уведомлений входят уведомления со статусом *Не просмотрено*.

Вы можете контролировать сеть вашей организации, просматривая уведомления на экране (см. стр. 1442) и отвечая на них в режиме реального времени.

**Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта**

Kaspersky Security Center позволяет вам контролировать сеть вашей организации, отправляя уведомления о событиях, которые вы считаете важными. Для любого события вы можете настроить уведомления по электронной почте, SMS или запустив исполняемый файл или скрипт (см. стр. 1450).

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

## Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг и отчеты** → **Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В веб-виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг и отчетность** → **Панель мониторинга**. В этом веб-виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

► *Чтобы просмотреть уведомления предопределенной категории:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.

2. На левой панели выберите одну из следующих категорий:

   - **Развертывание.**
   - **Устройства.**
   - **Защита.**
   - **Обновления** (сюда входят уведомления о доступных для загрузки программах "Лаборатории Касперского" и уведомления о загруженных обновлениях антивирусных баз).
   - **Защита от эксплойтов.**
   - **Сервер администрирования** (это уведомление включает в себя события, относящиеся только к Серверу администрирования).
   - **Полезные ссылки** (сюда входят ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию).
   - **Корпоративные новости "Лаборатории Касперского"** (сюда входит информация о выпусках программ "Лаборатории Касперского").

   В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления** ( ), **Предупреждающие уведомления** ( ), **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.
- **Уведомление**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу (см. стр. 1038) и установить программу безопасности на устройства, просмотреть список устройств или список событий. После того, как вы выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.
- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

► *Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:*

1. Нажмите на значок флага () в правом верхнем углу Kaspersky Security Center 14.2 Web Console.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана закладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите закладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* ( ) и *Предупреждающие уведомления* (). Список уведомление включает следующее:

   - Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
   - Значок, относящийся к теме уведомления: развертывание (), защита (), обновления(), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
   - Описание уведомления.
   - Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
   - Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
   - Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите закладку **Информационное сообщение**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на закладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

► *Чтобы просмотреть экранные уведомления на веб-виджете:*

1. В разделе **Панель мониторинга** нажмите на кнопку **Добавить или восстановить веб-виджет**.
2. В открывшемся окне нажмите на категорию **Другое**, выберите веб-виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить (см. стр. 1364).

   Веб-виджет отображается на закладке **Панель мониторинга**. По умолчанию на веб-виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на веб-виджете и изменить параметры веб-виджета (см. стр. 1365), чтобы просмотреть уведомления с уровнем важности *Предупреждающие уведомления*. Или вы можете добавить другой веб-виджет: **Уведомления, выбранные по уровню важности** с уровнем важности *Предупреждающие уведомления*.

   Список уведомлений на веб-виджете ограничен размером и включает только два уведомления. Эти два уведомления относятся к последним событиям.

Список уведомлений веб-виджета включает следующее:

- Значок, относящийся к теме уведомления: развертывание (), защита (), обновления (), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
- Описание уведомления со ссылкой на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
- Количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.
- Ссылка на другие уведомления. Перейдите по ссылке к просмотру уведомлений в разделе **Уведомления** раздела **Мониторинг и отчеты**.

## О статусах устройства

Kaspersky Security Center присваивает статус каждому управляемому устройству. Конкретный статус зависит от того, выполнены ли условия, определенные пользователем. В некоторых случаях при присваивании статуса устройству Kaspersky Security Center учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center не находит устройство в сети в течение двух часов, видимость устройства принимает значение *Не в сети*.

Существуют следующие статусы:

- *Критический* или *Критический / Видим в сети*.
- *Предупреждение* или *Предупреждение / Видим в сети*.
- *ОК* или *ОК / Видим в сети*.

В таблице ниже приведены условия по умолчанию для присвоения устройству статуса *Критический* или *Предупреждение* и их возможные значения.

*Таблица 102. Условия присвоения статусов устройству*

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Не установлена программа безопасности | Агент администрирования установлен на устройстве, но не установлена программа безопасности. | • Переключатель включен.<br>• Переключатель выключен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Найдено много вирусов | В результате работы задач поиска вирусов, например, задачи *Поиск вредоносного ПО*, на устройстве найдены вирусы, и количество обнаруженных вирусов превышает указанное значение. | Более 0. |
| Уровень постоянной защиты отличается от уровня, установленного администратором | Устройство видимо в сети, но уровень постоянной защиты отличается от уровня, установленного администратором в условии для статуса устройства. | • Остановлена.<br>• Приостановлена.<br>• Выполняется. |
| Давно не выполнялся поиск вредоносного ПО | Устройство видимо в сети и на устройстве установлена программа безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее. | Более 1 дня. |
| Базы устарели | Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее. | Более 1 дня. |
| Давно не подключались | Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено. | Более 1 дня. |
| Обнаружены активные угрозы | Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение. | Более чем 0 штук. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Требуется перезагрузка | Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин. | Более чем 0 минут. |
| Установлены несовместимые программы | Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы. | • Переключатель выключен.<br>• Переключатель включен. |
| Обнаружены уязвимости в программах | Устройство видимо в сети, и на нем установлен Агент администрирования, но в результате выполнения задачи *Поиск уязвимостей и требуемых обновлений* на устройстве обнаружены уязвимости в программах с заданным уровнем критичности. | • Предельный.<br>• Высокий.<br>• Средний.<br>• Игнорировать, если нельзя закрыть уязвимость.<br>• Игнорировать, если обновление назначено к установке. |
| Срок действия лицензии скоро истечет | Устройство видимо в сети, но срок действия лицензии истек. | • Переключатель выключен.<br>• Переключатель включен. |
| Срок действия лицензии истекает | Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней. | Более чем 0 дней. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| Давно не выполнялась проверка обновлений Центра обновления Windows | Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени. | Более 1 дня. |
| Недопустимый статус шифрования | Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению. | • Не соответствует политике из-за отказа пользователя (только для внешних устройств).<br>• Не соответствует политике из-за ошибки.<br>• В процессе применения политики – требуется перезагрузка.<br>• Не задана политика шифрования.<br>• Не поддерживается.<br>• В процессе применения политики. |
| Параметры мобильного устройства не соответствуют политике | Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия. | • Переключатель выключен.<br>• Переключатель включен. |
| Есть необработанные инциденты | На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором. | • Переключатель выключен.<br>• Переключатель включен. |
| Статус устройства определен программой | Статус устройства определяется управляемой программой. | • Переключатель выключен.<br>• Переключатель включен. |

| Условие | Описание условия | Доступные значения |
|---|---|---|
| На устройстве заканчивается дисковое пространство | Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению. | Более чем 0 МБ. |
| Устройство стало неуправляемым | Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования. | • Переключатель выключен.<br>• Переключатель включен. |
| Защита выключена | Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени. | Более чем 0 минут. |
| Программа безопасности не запущена | Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена. | • Переключатель выключен.<br>• Переключатель включен. |

Kaspersky Security Center позволяет настроить автоматическое переключение статуса устройства в группе администрирования при выполнении заданных условий. При выполнении заданных условий клиентскому устройству присваивается один из статусов: *Критический* или *Предупреждение*. При невыполнении заданных условий клиентскому устройству присваивается статус *ОК*.

Разным значениям одного условия могут соответствовать разные статусы. Например, по умолчанию при соблюдении условия **Базы устарели** со значением **Более 3 дней** клиентскому устройству присваивается статус *Предупреждение*, а со значением **Более 7 дней** – статус *Критический*.

Если вы обновляете Kaspersky Security Center с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

См. также:

Настройка переключения статусов устройств .....1449

## Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

► *Чтобы изменить статус устройства на* Критический*:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В открывшемся окне свойств выберите закладку **Статус устройства**.
4. Выберите **Критический**.
5. В блоке **Установить статус "Критический"** включите условие, чтобы переключить устройство в состояние *Критическое*.

   Однако вы можете изменить параметры, которые не заблокированы в родительской политике.
6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.
9. Нажмите на кнопку **ОК**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

► *Чтобы изменить статус устройства на* Предупреждение*:*

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В открывшемся окне свойств выберите закладку **Статус устройства**.
4. Выберите **Предупреждение**.
5. В блоке **Установить статус "Предупреждения"**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   Однако вы можете изменить параметры, которые не заблокированы в родительской политике.
6. Установите переключатель рядом с условием в списке.
7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.

   Не для всех условий можно задать значения.

9. Нажмите на кнопку **ОК**.

При невыполнении заданных условий управляемому устройству присваивается статус *Предупреждение*.

## См. также:



## Настройка параметров доставки уведомлений

Вы можете настроить уведомления о событиях, возникающих в Kaspersky Security Center. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события программа Kaspersky Security Center посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события программа Kaspersky Security Center посылает уведомления на указанные номера телефонов.
- Исполняемый файл – при возникновении события исполняемый файл запускается на Сервере администрирования.

► *Чтобы настроить параметры доставки уведомлений о событиях, возникших в Kaspersky Security Center:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на закладке **Общие**.

2. Перейдите в раздел **Уведомления** и на правой панели выберите закладку с требуемым способом уведомления:

   - **Электронная почта**

     На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

     - IPv4-адрес или IPv6-адрес
     - Имя устройства в сети Windows (NetBIOS-имя)
     - DNS-имя SMTP-сервера

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

     Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени

SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

  Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

  Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата Сервера**

  Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выберите значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат для TLS подключения, перейдя по ссылке **Задать сертификаты**:

- Выберите файл сертификата SMTP-сервера:

  Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

- Выберите файл сертификата клиента:

  Вы можете использовать сертификат, полученный из любого источника, например, от любого аккредитованного центра сертификации. Вы должны указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

  - Сертификат X-509:

  Вы должны указать файл с сертификатом и файл с закрытым ключом. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла загружены, необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - Контейнер с сертификатом в формате PKCS#12:

  Вы должны загрузить один файл, содержащий сертификат и закрытый ключ сертификата. Когда файл загружен, тогда необходимо указать пароль для расшифровки закрытого ключа. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

В поле **Тема** укажите тему электронной почты. Вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашей электронной почты. Переменная, в соответствии с выбранным шаблоном, автоматически отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры (см. стр. 321) с подробными данными события.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

- **SMS**

  На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

  В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы

можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес
- Имя устройства в сети Windows (NetBIOS-имя)
- DNS-имя SMTP-сервера

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

  Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

  Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата Сервера**

  Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выберите значение **Всегда использовать TLS, для проверки срока действия сертификата Сервера**, вы можете указать сертификат для аутентификации SMTP-сервера и выбрать, хотите ли вы разрешить подключение через любую версию TLS или только через TLS 1.2 или более поздние версии. Также вы можете указать сертификат для аутентификации клиента на SMTP-сервере.

Вы можете указать сертификат SMTP-сервера для TLS подключения, перейдя по ссылке **Задать сертификаты**:

Вы можете получить файл со списком сертификатов от аккредитованного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также аккредитованным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от аккредитованного центра сертификации.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой. Уведомления доставляются на телефоны, номера которых связаны с указанными адресами электронной почты.

В поле **Тема** укажите тему электронной почты.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы вашей электронной почты. Переменная, в соответствии с выбранным шаблоном, отображается в поле **Тема**. Вы можете создать тему электронной почты, выбрав несколько шаблонов темы.

В окне **Адрес электронной почты отправителя** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый программой при возникновении события. Текст может содержать подстановочные параметры (см. стр. 321), такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения указанным получателям.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

  В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится. Перед указанием файла подготовьте файл и укажите подстановочные параметры (см. стр. 321), которые определяют сведения о событии, которые будут отправлены в сообщении. Указанные папка и файл должны находиться на Сервере администрирования.

  При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

3. На закладке настройте параметры уведомлений.
4. Нажмите на кнопку **ОК**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky Security Center.

Можно изменить значения параметров доставки уведомлений (см. стр. 1175) для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах программы.

См. также:

Сценарий: Мониторинг и отчеты .....1360

## Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center позволяет с помощью запуска исполняемого файла уведомлять администратора о событиях на клиентских устройствах. Исполняемый файл должен содержать другой исполняемый файл с подстановочными параметрами события, которые нужно передать администратору.

*Таблица 103. Подстановочные параметры для описания события*

| Подстановочный параметр | Описание подстановочного параметра |
|---|---|
| %SEVERITY% | Уровень важности события |
| %COMPUTER% | Имя устройства, на котором произошло событие |
| %DOMAIN% | Доменная |
| %EVENT% | Событие |
| %DESCR% | Описание события |
| %RISE_TIME% | Время возникновения |
| %KLCSAK_EVENT_TASK_DISPLAY_NAME% | Имя задачи |
| %KL_PRODUCT% | Агент администрирования Kaspersky Security Center |
| %KL_VERSION% | Номер версии Агента администрирования |
| %HOST_IP% | IP-адрес; |
| %HOST_CONN_IP% | IP-адрес соединения |

**Пример:**

Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

# Объявления "Лаборатории Касперского"

Включение объявлений «Лаборатории Касперского» ведет к выходу программ из безопасного состояния программы.

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

## В этом разделе



## Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"** предоставляет информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. Kaspersky Security Center периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Kaspersky Security Center показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и программам "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

  Объявления, связанные с безопасностью, предназначены для того, чтобы программы "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для программ "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в программах "Лаборатории Касперского". Объявления, связанные с безопасностью, включены по умолчанию. Если вы не хотите получать объявления, вы можете отключить эту функцию.

  Чтобы показать вам информацию, которая соответствует вашей конфигурации защиты сети, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает только те объявления, которые относятся к программам "Лаборатории Касперского", установленным в вашей сети. Данные, которые могут быть отправлены на серверы, описаны в Лицензионном соглашении (см. стр. 343), которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

Рекламные объявления включают информацию о специальных предложениях для ваших программ "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN (см. стр. 829).

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Важная новость.
3. Предупреждение.
4. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" программа Kaspersky Security Center 14.2 Web Console отображает метку уведомления, соответствующую уровню важности объявлений. Вы можете нажать на метку, чтобы просмотреть это объявление в разделе Объявления "Лаборатории Касперского".

Вы можете указать параметры объявлений "Лаборатории Касперского" (см. стр. 1457), включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления.

### См. также:



## Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и где отображать метку уведомления.

► *Чтобы настроить объявления "Лаборатории Касперского":*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Объявления "Лаборатории Касперского"**.
2. Перейдите по ссылке **Параметры**.

   Откроется окно объявлений "Лаборатории Касперского".
3. Задайте следующие параметры:
   - Выберите уровень важности объявлений, которые вы хотите просматривать. Объявления других категорий отображаться не будут.
   - Выберите расположение, где вы хотите видеть метку уведомления. Метка может отображаться во всех разделах консоли или в разделе **Мониторинг и отчеты** и его подразделах.
4. Нажмите на кнопку **ОК**.

Параметры объявлений "Лаборатории Касперского" настроены.

## См. также:



## Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Объявления "Лаборатории Касперского" включают в себя информацию двух типов: объявления, связанные с безопасностью, и рекламные объявления. Вы можете выключить объявления каждого типа отдельно.

► *Чтобы выключить объявления, связанные с безопасностью:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.
3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.
4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Рекламные объявления по умолчанию выключены. Вы получаете рекламные сообщения только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить этот тип объявлений, отключив KSN.

► *Чтобы отключить объявления:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. Выключите параметр **Использовать Kaspersky Security Network Включено**.
4. Нажмите на кнопку **Сохранить**.

   Объявления выключены.

## См. также:

kaspersky

# Просмотр информации об обнаруженных угрозах

Вы можете включить или отключить отображение информации об обнаружениях.

► *Чтобы включить или выключить отображение раздела **Обнаружения** в главном меню:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.
2. В появившемся окне **Параметры интерфейса** выключите параметр **Показать EDR-обнаружения**.
3. Нажмите на кнопку **Сохранить**.

В консоли отображается раздел **Обнаружения** в разделе **Мониторинг и отчеты** главного меню. В разделе **Обнаружения** вы можете просматривать информацию об обнаруженных угрозах на устройствах. Если вы добавите лицензионный ключ для EDR Optimum https://support.kaspersky.com/KEDR_Optimum/2.3/ru-RU/220194.htm, Kaspersky Security Center 14.2 Web Console автоматически отобразит подраздел **Обнаружения** в главном меню в разделе **Мониторинг и отчеты**. Также вы можете добавить веб-виджет (см. стр. 1364), в котором отображается информация об обнаружениях. Если вы установили плагин EDR Optimum, вы можете просмотреть подробную информацию об обнаруженных угрозах по ссылке **Подробнее**.

Используйте меню **Фильтр**, чтобы отфильтровать обнаружения по дате и значениям поля.

Поле **Тип объекта** содержит одно из следующих значений:

- неизвестно;
- фишинговая ссылка;
- вирус;
- троянская программа;
- вредоносные утилиты;
- троянская программа удаленного администрирования;
- червь;
- другая программа;
- рекламные программы;
- порнографическая программа;
- опасно упакованная программа;
- опасное поведение.

Поле **Автоматический ответ** содержит одно из следующих значений:

- Обнаружен вредоносный объект;
- Объект удален;
- Объект вылечен;
- Не удалось вылечить объект;
- Объект помещен на карантин;
- Обнаружен архив, защищенный паролем;
- Обнаружен вирус.

kaspersky

См. также:

Сценарий: Мониторинг и отчеты .....1360

# Загрузка и удаление файлов из Карантина и Резервного хранилища

В этом разделе представлена информация о том, как загрузить и удалить файлы из Карантина и Резервного хранилища в Kaspersky Security Center 14.2 Web Console.

См. также:

Карантин и резервное хранилище .....824

## Загрузка файлов из Карантина и Резервного хранилища

Вы можете загрузить файлы из Карантина и Резервного хранилища, только если выполняется одно из двух условий: либо включен параметр **Не разрывать соединение с Сервером администрирования** в свойствах устройства, либо используется шлюз соединения. Иначе загрузка невозможна.

► *Чтобы сохранить копию файла из карантина или резервного хранилища на жесткий диск, выполните следующие действия:*

1. Выполните одно из следующих действий:
   - Если вы хотите сохранить копию файла из Карантина, в главном меню перейдите в раздел **Операции → Хранилища → Карантин**.
   - Если вы хотите сохранить копию файла из Резервного хранилища, в главном меню перейдите в раздел **Операции → Хранилища → Резервное хранилище**.
2. В открывшемся окне выберите файл, который вы хотите загрузить, и нажмите **Загрузить**.

Начнется загрузка. Копия файла, помещенного в Карантин на клиентском устройстве, сохраняется в указанную папку.

См. также:

Карантин и резервное хранилище .....824

## Об удалении объектов из Карантина, Резервного хранилища или Активных угроз

Когда программы безопасности "Лаборатории Касперского", установленные на клиентских устройствах, помещают объекты на Карантин, в Резервное хранилище или Активные угрозы, они передают информацию о добавленных объектах в разделы **Карантин**, **Резервное хранилище** или **Активные угрозы** в Kaspersky Security Center. При открытии одного из этих разделов выберите объект из списка и нажмите на кнопку **Удалить**, Kaspersky Security Center выполняет одно из следующих действий или оба действия:

- Удаляет выбранный объект из списка.
- Удаляет выбранный объект из хранилища.

Действие, которое необходимо выполнить, определяется программой "Лаборатории Касперского", поместившей выбранный объект в хранилище. Программа "Лаборатории Касперского" указана в поле **Запись добавлена**. Подробную информацию о том, какое действие необходимо выполнить, см. в документации к программе "Лаборатории Касперского".

### См. также:

Карантин и резервное хранилище .....824

# Журнал активности Kaspersky Security Center 14.2 Web Console

Журнал активности Kaspersky Security Center 14.2 Web Console может помочь выяснить причины сбоя программного обеспечения. Когда вы обращаетесь в Службу технической поддержки "Лаборатории Касперского" в случае сбоя Kaspersky Security Center 14.2 Web Console, специалисты Службы технической поддержки могут попросить у вас файлы журнала событий Kaspersky Security Center 14.2 Web Console. Файлы журнала Kaspersky Security Center 14.2 Web Console хранятся в папке <Папка установки Kaspersky Security Center 14.2 Web Console>/logs все время использования программы. Файлы журнала не отправляются автоматически специалистам Службы технической поддержки "Лаборатории Касперского".

► *Чтобы включить журнал активности Kaspersky Security Center 14.2 Web Console,*

Установите флажок **Включить запись в журнал Kaspersky Security Center Web Console** в окне **Параметры подключения Kaspersky Security Center Web Console** мастера установки Kaspersky Security Center 14.2 Web Console (см. стр. 950).

Файлы журнала записываются в текстовом формате.

Имена файлов журнала записываются в формате -<имя компонента>.<имя устройства>-<номер ревизии файла>.ГГГГ-ММ-ДД, где

- <имя компонента> – имя компонента Kaspersky Security Center или имя плагина управления Kaspersky Security Center 14.2 Web Console.
- <имя устройства> – имя устройства, на котором запущен компонент или плагин (<имя компонента>).
- <номер ревизии файла> – номер файла журнала, созданного для компонента или плагина <имя компонента>, который запущен на устройстве <имя устройства>. В течение одного дня можно создать несколько файлов журнала для одного и того же компонента или плагина (<имя компонента>) и устройства (<имя устройства>). Максимальный размер файла журнала составляет 50 МБ. При достижении максимального размера файла создается новый файл журнала. Новый файл журнала (<номер ревизии файла>) увеличивается на 1.
- ГГГГ, ММ, и ДД это год, месяц и день, когда была создана первая запись журнала. Новый файл журнала создается, когда начинается новый день.

kaspersky

# Интеграция Kaspersky Security Center с другими решениями

В этом разделе описывается, как настроить доступ из Kaspersky Security Center Web Console к другой программе "Лаборатории Касперского", например Kaspersky Endpoint Detection and Response и Kaspersky Managed Detection and Response. Также описано как настроить экспорт событий в SIEM-системы.

## В этом разделе



## Настройка доступа к веб-консоли KATA/KEDR

Kaspersky Anti Targeted Attack (KATA) и Kaspersky Endpoint Detection and Response (KEDR) это два функциональных блока программы Kaspersky Anti Targeted Attack Platform https://help.kaspersky.com/KATA/3.7.2/ru-RU/. Вы можете управлять этими функциональными блоками с помощью веб-консоли для Kaspersky Anti Targeted Attack Platform (веб-консоль KATA / KEDR). Если вы используете и Kaspersky Security Center 14.2 Web Console и веб-консоль KATA / KEDR, вы можете настроить доступ к веб-консоли KATA / KEDR напрямую через интерфейс программы Kaspersky Security Center 14.2 Web Console.

► *Чтобы настроить доступ к веб-консоли KATA / KEDR:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Интеграция**.
2. На закладке **Интеграция** выберите раздел **KATA**.
3. Укажите веб-адрес веб-консоли KATA / KEDR в поле **Веб адрес веб-консоли KATA / KEDR**.
4. Нажмите на кнопку **Сохранить**.

Раскрывающийся список **Расширенное управление** добавляется в верхнюю часть главного окна программы. Вы можете использовать это меню, чтоб открывать веб-консоль KATA / KEDR. После того, как вы нажмете **Advanced Cybersecurity**, в вашем браузере откроется новая закладка с указанным вами веб-адресом.

## См. также:


Сценарий:Обновление Kaspersky Security Center и управляемых программ безопасности ..... 280


## Установка фонового соединения

Чтобы программа Kaspersky Security Center 14.2 Web Console могла выполнять свои фоновые задачи, вам необходимо установить соединение между Kaspersky Security Center Web Console и Сервером администрирования. Вы можете установить это соединение, только если в вашей учетной записи есть право **Изменение списков управления доступом объектов** (см. стр. 771) в функциональной области **Общий функционал**: **Права пользователей**.

Если вы устанавливаете плагин Kaspersky Endpoint Security для Windows 11.5.0 или обновляете плагин Kaspersky Endpoint Security для Windows с версии ниже 11.7 и фоновое соединение еще не установлено, отображается уведомление о том, что необходимо установить фоновое соединение. Также вам нужно будет

предоставить учетной записи службы права **Общий функционал**: функциональная область **Операции с Сервером администрирования** (см. стр. 771).

► *Чтобы установить фоновое соединение:*

1. В главном окне программы перейдите в раздел **Параметры консоли** → **Интеграция**.
2. На закладке **Интеграция** переключите переключатель установки фонового соединения в положение: **Установить фоновое соединения для интеграции**.
3. В разделе **Установить фоновое соединение** нажмите на кнопку **ОК**.

Фоновое соединение между Kaspersky Security Center Web Console и Сервером администрирования установлено. Сервер администрирования создает учетную запись для фонового подключения, и эта учетная запись используется как служебная учетная запись для поддержания взаимодействия Kaspersky Security Center с другой программой или решением "Лаборатории Касперского". Имя этой учетной записи службы содержит префикс NWCSvcUser.

Сервер администрирования автоматически меняет пароль учетной записи службы каждые 30 дней в целях безопасности. Вы не можете удалить учетную запись службы вручную. Сервер администрирования автоматически удаляет эту учетную запись при отключении соединения. Сервер администрирования создает единую учетную запись службы для каждой Консоли администрирования и назначает все учетные записи службы группе безопасности с именем ServiceNwcGroup. Сервер администрирования создает эту группу безопасности автоматически в процессе установки Kaspersky Security Center. Вы не можете удалить эту группу безопасности вручную.

### См. также:

Сценарий:Обновление Kaspersky Security Center и управляемых программ безопасности .....280

Основной сценарий установки.....92

# Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров программы;
- загрузки журналов событий;
- создания файла дампа для программы;
- загрузки диагностики и загрузки результатов диагностики;
- запуска, остановка и перезапуск программ.

Вы можете использовать журнал событий и диагностические отчеты, загруженные с клиентского устройства, для устранения неполадок самостоятельно. Также если вы обращаетесь в Службу технической поддержки "Лаборатории Касперского", специалист технической поддержки "Лаборатории Касперского" может попросить вас загрузить файлы трассировки, файлы дампа, журнал событий и диагностические отчеты с клиентского устройства для дальнейшего анализа в "Лаборатории Касперского".

Удаленная диагностика выполняется с использованием Сервера администрирования.

kaspersky

## В этом разделе



# Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентского устройства, сначала нужно открыть окно удаленной диагностики.

► *Чтобы открыть окно удаленной диагностики:*

1. Чтобы выбрать устройство, для которого вы хотите открыть окно удаленной диагностики, выполните одно из следующих действий:
   - Если устройство принадлежит к группе администрирования, в главном меню перейдите в раздел **Устройства** → **Управляемые устройства**.
   - Если устройство принадлежит к группе нераспределенных устройств, в главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Нераспределенные устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите закладку **Дополнительно**.
4. В появившемся окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства.

См. также:



# Включение и выключение трассировки для программ

Вы можете включать и выключать трассировку для программ, включая трассировку xperf.

**Включение и выключение трассировки**

► *Чтобы включить или выключить трассировку на удаленном устройстве:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.
4. В дереве объектов устройства выберите программу, для которой требуется включить или выключить трассировку.

   Отображается список параметров удаленной диагностики.
5. Если вы хотите включить трассировку:
   a. В разделе **Трассировка**, нажмите на кнопку **Включить трассировку**.
   b. В открывшемся окне **Изменить уровень трассировки** рекомендуется не менять значения, заданные по умолчанию. При необходимости специалист Службы технической поддержки проведет вас через процесс настройки. Доступны следующие параметры:

      - **Уровень трассировки**

Уровень трассировки определяет состав информации, которую содержит файл трассировки.

      - **Трассировка на основе ротации**

Программа перезаписывает информацию трассировки, чтобы предотвратить чрезмерное увеличение файла трассировки. Укажите максимальное количество файлов, которые будут использоваться для хранения информации трассировки, и максимальный размер каждого файла. Если записано максимальное количество файлов трассировки максимального размера, самый старый файл трассировки будет удален, чтобы можно было записать новый файл трассировки.

Этот параметр доступен только для Kaspersky Endpoint Security.

a. Нажмите на кнопку **Сохранить**.

Трассировка включена для выбранной программы. В некоторых случаях для включения трассировки программы безопасности требуется перезапустить эту программу и ее задачу.

1. Если вы хотите выключить трассировку для выбранной программы, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранной программы.

**Включение трассировки Xperf**

Для Kaspersky Endpoint Security специалисты Службы технической поддержки могут попросить вас включить трассировку Xperf для получения информации о производительности системы.

► *Чтобы включить и настроить трассировку Xperf:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.
4. В списке программ выберите Kaspersky Endpoint Security для Windows.

   Отображается список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.
5. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**.
6. В открывшемся окне **Изменить уровень трассировки Xperf**, в зависимости от запроса специалиста Службы технической поддержки, выполните следующее:

   a. Выберите один из уровней трассировки:

   - **Легкий уровень**

     Файл трассировки этого типа содержит минимальный объем информации о системе.

     По умолчанию выбран этот вариант.

   - **Детальный уровень**

     Файл трассировки этого типа содержит более подробную информацию, чем файл типа *Легкий уровень*, и может запрашиваться специалистами Технической поддержки, если информации в файле трассировки *легкого уровня* недостаточно для оценки производительности. Файл трассировки *Детального уровня* содержит информацию об оборудовании, операционной системе, список запущенных и завершенных процессов и программ, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

   b. Выберите один из уровней трассировки Xperf:

   - **Базовый тип**

     Программа получает данные трассировки во время работы программы Kaspersky Endpoint Security.

По умолчанию выбран этот вариант.

- **Тип перезагрузки**

  Программа получает данные трассировки, когда на управляемом устройстве запускается операционная система. Этот тип трассировки эффективен, когда проблема, влияющая на производительность системы, возникает после включения устройства и перед запуском Kaspersky Endpoint Security.

Также вам могут предложить включить параметр **Трассировка на основе ротации**, чтобы предотвратить чрезмерное увеличение файла трассировки. Затем укажите максимальный размер файла трассировки. Когда файл достигает максимального размера, самый старый файл трассировки будет перезаписан новым файлом.

c. Определите размер файла ротации.

d. Нажмите на кнопку **Сохранить**.

Трассировка Xperf включена и настроена.

► *Чтобы выключить трассировку Xperf:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.
4. В списке программ выберите Kaspersky Endpoint Security для Windows.

   Отобразятся параметры трассировки для Kaspersky Endpoint Security для Windows.
5. В разделе **Трассировка Xperf**, нажмите на кнопку **Выключить трассировку Xperf**.

   Если трассировка Xperf уже выключена, отображается кнопка **Включить трассировку Xperf**.

Трассировка Xperf выключена.

## Загрузка файла трассировки программы

► *Чтобы загрузить файл трассировки программы:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.

   В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы событий трассировки устройства**, где отображается список файлов трассировки.
4. В списке файлов трассировки выберите требуемый файл.
5. Выполните одно из следующих действий:

- Загрузите выбранный файл, нажав на кнопку **Загрузить весь файл**.
- Загрузите часть выбранного файла:
  a. Нажмите на кнопку **Загрузить часть**.
  b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.
  c. Нажмите на кнопку **Загрузить**.

Выбранный файл или его часть загружается в указанное вами расположение.

## Удаление файлов трассировки

Вы можете удалить файлы трассировки, которые больше не нужны.

► *Чтобы удалить файл трассировки:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В появившемся окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В открывшемся окне **Статусы и журнал событий**, убедитесь, что выбран раздел **Журнал событий операционной системы**.
4. В разделе **Файлы трассировки** нажмите на кнопку **Журналы службы Центра обновления Windows** или на кнопку **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   Откроется список файлов трассировки.
5. В списке файлов трассировки выберите файл, который вы хотите удалить.
6. Нажмите на кнопку **Удалить**.

Выбранный файл трассировки будет удален.

## Загрузка параметров программ

► *Чтобы загрузить с клиентского устройства параметры программ:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В появившемся окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В открывшемся окне **Статусы и журнал событий**, убедитесь, что выбран раздел **Журнал событий операционной системы**.
   - В разделе **Информация о системе** нажмите на кнопку **Загрузить файл** для загрузки системной информации о клиентском устройстве.
   - В разделе **Параметры программы** нажмите на кнопку **Загрузить файл** для загрузки информации о параметрах программ, установленных на устройстве.

Информация загружается в папку, указанную вами, в виде файла.

## Загрузка журналов событий

► *Чтобы загрузить с удаленного устройства журнал событий:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Журнал событий устройства**.
3. В окне **Журнал событий всех устройств** выберите соответствующий журнал событий.
4. Выполните одно из следующих действий:
   - Загрузите выбранный журнал событий, нажав на кнопку **Загрузить весь файл**.
   - Загрузите часть выбранного журнала событий:
     a. Нажмите на кнопку **Загрузить часть**.
     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.
     c. Нажмите на кнопку **Загрузить**.

Выбранный журнал событий или его часть загружаются в указанное вами место.

## Запуск, остановка и перезапуск программы

Вы можете запускать, останавливать и перезапускать программы на клиентском устройстве.

► *Чтобы запустить, остановить или перезапустить программу:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.
4. В списке программ выберите программу, которую вы хотите запустить, остановить или перезапустить.
5. Выберите действие, нажав на одну из следующих кнопок:
   - **Остановить программу.**

     Эта кнопка доступна, только если программа в данный момент запущена.
   - **Перезапустить программу.**

     Эта кнопка доступна, только если программа в данный момент запущена.
   - **Запустить программу.**

     Эта кнопка доступна, только если программа в данный момент не запущена.

В зависимости от выбранного вами действия требуемая программа запустится, остановится или перезапустится на клиентском устройстве.

Если вы перезапустите Агент администрирования, появится сообщение о том, что текущее соединение устройства с Сервером администрирования будет потеряно.

## Запуск удаленной диагностики программы и загрузка результатов

► *Чтобы запустить диагностику программы на удаленном устройстве и загрузить ее результаты:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Программы "Лаборатории Касперского"**.

   Откроется список программ "Лаборатории Касперского", установленных на устройстве.
4. В списке программ выберите программу, для которой вы хотите запустить удаленную диагностику.

   Отображается список параметров удаленной диагностики.
5. В разделе **Отчет диагностики** нажмите на кнопку **Выполнить диагностику**.

   Запускается процесс удаленной диагностики и генерируется отчет о диагностике. По завершении процесса диагностики кнопка **Загрузить отчет диагностике** становится доступной.
6. Загрузите отчет, нажав кнопку на **Загрузить отчет диагностики**.

Отчет загружается в указанное вами место.

## Запуск программы на клиентском устройстве

Вам может потребоваться запустить программу на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского".

Вам не нужно устанавливать программу самостоятельно на этом устройстве.

► *Чтобы запустить программу на клиентском устройстве:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В появившемся окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Запуск удаленной программы**.
4. В окне **Запуск удаленной программы**, в разделе **Файлы программы** выполните одно из следующих действий в зависимости от того, что вас попросит сделать специалист "Лаборатории Касперского":
   - Выберите ZIP-архив с программой, которую вы хотите запустить на клиентском устройстве, нажав на кнопку **Обзор**.

     ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

   - Укажите программу командной строки и ее аргументы, если необходимо. Для этого заполните поля **Исполняемый файл в архиве для запуска на удаленном устройстве** и **Аргументы командной строки**.
5. Нажмите на кнопку **Загрузить и запустить**, чтобы запустить указанную программу на клиентском устройстве.

6. Следуйте далее указаниям специалиста.

## Создание файла дампа для программы

Файл дампа программы позволяет просматривать параметры программы, работающей на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для программы.

Создание файлов дампа доступно только для 32-разрядных процессов, работающих на клиентских устройствах под управлением Windows. Для 64-разрядных процессов эта функция не поддерживается.

► *Чтобы создать файл дампа для программы:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 1464).
2. В появившемся окне удаленной диагностики нажмите на кнопку **Удаленная диагностика**.
3. В отобразившемся окне **Статусы и журнал событий** выберите раздел **Запуск удаленной программы**.
4. В разделе **Формирование дампа процесса** укажите исполняемый файл программы, для которой вы хотите создать файл дампа.
5. Нажмите на кнопку **Загрузить дамп файла**, чтобы сохранить файл дампа указанной программы.

   Если указанная программа не запущена на клиентском устройстве, отобразится сообщение об ошибке.

kaspersky

# Настройка эталонных значений параметров программы Kaspersky Security Center Web Console

Этот раздел содержит инструкции по установке эталонных значений параметров программы Kaspersky Security Center Web Console. Настройка программы по эталонным параметрам необходима для работы сертифицированной конфигурации программы.

### Месторасположение папки общего доступа Сервера администрирования

Папка общего доступа не должна находиться в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа установленного Сервера администрирования:*

1. Выберите Сервер администрирования.
2. Нажмите на иконку **Свойства** (⚙).
3. На закладке **Общие** выберите **Папка общего доступа Сервера администрирования**.
4. В поле **Путь к папке общего доступа** измените расположение папки общего доступа.

Расположение **Папки общего доступа Сервера администрирования** изменится на указанное.

### Политики

Для политики Агента администрирования необходимо установить пароль на удаление программы Агента администрирования. Для политики Kaspersky Endpoint Security для Windows необходимо настроить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows. В политике Kaspersky Endpoint Security для Windows необходимо настроить отправку уведомлений по электронной почте при возникновении событий об обнаружении вредоносного ПО.

### Пароль на деинсталляцию Агента администрирования

Необходимо установить пароль на удаление программы Агента администрирования.

► *Чтобы установить пароль на деинсталляцию программы Агента администрирования:*

1. В разделе **Устройства** выберите **Политики и профили политик**.
2. Выберите политику Агента администрирования.

   Откроется окно свойств политики.
3. В окне свойств политики в разделе **Параметры программы** выберите подраздел **Параметры**.
4. Включите параметр **Использовать пароль деинсталляции**.
5. В поле **Пароль** введите пароль на деинсталляцию программы.
6. Нажмите на кнопку **Сохранить**.

Пароль на удаление программы Агента администрирования установлен.

### Защита паролем политики Kaspersky Endpoint Security для Windows

Необходимо установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows.

► *Чтобы установить защиту паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows:*

1. На закладке **Устройства** выберите **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.
3. В окне свойств политики в разделе **Дополнительные параметры** выберите подраздел **Параметры программы**.
4. В разделе **Параметры программы** в блоке **Защита паролем** нажмите на кнопку **Настроить**.
5. В окне **Защита паролем** установите флажок **Включить защиту паролем**.
6. В окне **Защита паролем** в блоке **Область действия пароля** установите флажок **Удаление / Изменение / Восстановление программы**.
7. Нажмите на кнопку **ОК**.

Защита паролем на удаление, изменение или восстановление программы Kaspersky Endpoint Security для Windows установлена.

**Автоматическое обновление модулей Агентов администрирования**

По умолчанию обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Необходимо отключить автоматическое обновление модулей Агента администрирования. Сертификации подлежат только определенные версии исполняемых модулей программы.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера Администрирования**.

   Откроется окно свойств задачи.
3. В окне задачи выберите раздел **Параметры программы**.
4. В разделе **Прочие настройки** выберите **Прочие параметры** и перейдите по ссылке **Настроить**.

   Откроется окно параметров.
5. Выключите параметр **Обновлять модули Агентов администрирования**.

   Если параметр выключен, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
6. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей программы отключено.

Если в сети вашей организации назначены точки распространения, то для всех точек распространения также требуется отключить автоматическое обновление модулей Агента администрирования.

► *Чтобы отключить автоматическое обновление исполняемых модулей программы точкой распространения:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилища точек распространения**.

В результате откроется окно свойств задачи.

3. В окне задачи выберите раздел **Параметры программы**.
4. Выключите параметр **Обновлять модули Агентов администрирования**.

   Если параметр выключен, автоматическая установка обновлений не выполняется. Полученные обновления модулей Агента администрирования можно установить вручную.
5. Нажмите на кнопку **ОК**.

Автоматическое обновление исполняемых модулей программы точкой распространения отключено.

**Установка применимых обновлений со статусом одобрения "Не определено"**

По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Необходимо отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

► *Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения* Не определено:

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику Агента администрирования.

   Откроется окно свойств политики.
3. В открывшемся окне свойств политики выберите закладку **Параметры и программы**.
4. Выберите раздел **Управление патчами и обновлениями** снимите флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"**.
5. Если флажок **Автоматически устанавливать применимые обновления и патчи для компонентов со статусом "Не определено"** снят, загруженные патчи "Лаборатории Касперского" со статусом *Не определено* устанавливаются после того, как администратор изменит их статус на *Одобрен*.
6. Нажмите на кнопку **Сохранить**.

Автоматическая установка патчей "Лаборатории Касперского" со статусом одобрения *Не определено отключено.*

Запуск задач Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Необходимо настроить автоматический запуск задач **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**.

Рекомендуемый интервал автоматического запуска задач Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения** составляет один раз в час.

► *Чтобы настроить автоматический запуск задачи Сервера администрирования* ***Загрузка обновлений в хранилище Сервера администрирования*** *один раз в час:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.

   Откроется окно свойств задачи.

3. В окне свойств выберите закладку **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.
5. В поле **Интервал запуска (ч)** установите значение 1.
6. Нажмите на кнопку **Сохранить**.

Автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** один раз в час настроен.

Если в сети организации назначены точки распространения, необходимо также настроить автоматический запуск задачи **Загрузка обновлений в хранилища точек распространения**. Для этого необходимо повторить действия, описанные выше для задачи **Загрузка обновлений в хранилище Сервера администрирования**.

**Запуск задачи** Установка обновлений

После выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** необходимо настроить запуск задачи **Установка обновлений**.

► *Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования**:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Установка обновлений**.

   В результате откроется окно свойств задачи.
3. В окне свойств выберите закладку **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **По завершении другой задачи**.
5. В поле **Результат выполнения** выберите значение **Завершена успешно**.
6. В поле **Имя** выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
7. Нажмите на кнопку **Сохранить**.

   Автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** настроен.

**Передача данных службе KSN**

Kaspersky Security Network (KSN) – это инфраструктура онлайн-служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний (см. стр. 829).

Для работы программы в сертифицированной конфигурации службы, которые связаны с отправкой данных на внешние сервера и получением команд от внешних серверов (за периметром сети организации), должны быть отключены.

► *Чтобы отключить передачу данных службе KSN:*

1. Выберите Сервер администрирования, для которого нужно отключить передачу данных к службе KSN.
2. Нажмите на кнопку **Свойства**.

3. В результате откроется окно свойств Сервера администрирования.
4. В окне свойств Сервера администрирования на закладке **Общие** выберите **Параметры прокси-сервера KSN**.
5. Снимите флажок **Я принимаю условия использования Kaspersky Security Network**, чтобы выключить автоматическую передачу данных "Лаборатории Касперского" о работе установленных на устройствах программ "Лаборатории Касперского".
6. При необходимости снимите флажок **Использовать Сервер администрирования как прокси-сервер**, чтобы выключить службу прокси-сервера KSN.
7. Нажмите на кнопку **Сохранить**.

Если флажок снят, передача данных в KSN от Сервера администрирования и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

► *Чтобы отключить передачу данных службе KSN точкой распространения:*

1. Выберите Сервер администрирования, для которого нужно отключить передачу данных к службе KSN.
2. Нажмите на кнопку **Свойства**.
3. В результате откроется окно свойств Сервера администрирования.
4. В окне свойств Сервера администрирования на закладке **Общие** выберите **Точки распространения**.
5. В поле **Устройство** выберите нужное устройство.

   Откроется окно свойств точки распространения,
6. В окне свойств точки распространения выберите раздел **Прокси-сервер KSN**.
7. Выключите параметр **Включить прокси-сервер KSN на стороне точек распространения**, чтобы выключить службу прокси-сервера KSN.
8. Нажмите на кнопку **ОК**.

Если флажок снят, передача данных в KSN от точки распространения и от клиентских устройств через Kaspersky Security Center не осуществляется. При этом клиентские устройства в соответствии со своими параметрами могут передавать данные в KSN напрямую (не через Kaspersky Security Center). Действующая на клиентских устройствах политика Kaspersky Endpoint Security для Windows определяет, какие данные эти устройства напрямую (не через Kaspersky Security Center) передают в KSN.

Передача данных службе KSN должна быть отключена во всех управляемых программах.

Альтернативой отказу от использования KSN может стать использование Локального KSN (см. стр. 830). В этом случае вы получите доступ к оперативной базе знаний "Лаборатории Касперского", но информация о работе программ "Лаборатории Касперского" не будет передаваться на сервера "Лаборатории Касперского". Подробнее см. в разделе Kaspersky Security Network (KSN) (на стр. 829).

.Источник обновлений задачи Загрузка обновлений в хранилище и задачи **Загрузка обновлений в хранилища точек распространения**

Для отключения передачи данных программой серверу обновлений "Лаборатории Касперского" необходимо удалить серверы обновлений "Лаборатории Касперского" в задачах **Загрузка обновлений в хранилище Сервера администрирования** и **Загрузка обновлений в хранилища точек распространения**.

► *Чтобы удалить серверы обновлений "Лаборатории Касперского" в задаче Загрузка обновлений в хранилище Сервера администрирования из источников обновлений:*

1. На закладке **Устройства** выберите **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
3. В окне свойств задачи перейдите в раздел **Параметры программы**.
4. В подразделе **Источники обновлений** перейдите по ссылке **Настроить**.
5. В окне **Источники обновлений** удалите значение *Серверы обновлений "Лаборатории Касперского"*.
6. Нажмите на кнопку **ОК**.

Настройку необходимо выполнить для задачи **Загрузка обновлений в хранилище Сервера администрирования** и для задачи **Загрузка обновлений в хранилища точек распространения** для всех точек распространения.

**Способ активации Сервера администрирования**

Сервер администрирования необходимо активировать только при помощи файлов ключа.

► *Чтобы активировать Сервер администрирования с помощью файла ключа:*

1. Выберите Сервер администрирования, который вы хотите активировать.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Сервера администрирования.
3. В открывшемся окне свойств Сервера администрирования выберите закладку **Общие** → **Лицензионные ключи**.
4. В поле **Действующая лицензия** укажите файл ключа, на основании которого ключ будет добавлен в программу.
5. Нажмите на кнопку **ОК**.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации программы с помощью кода активации программа регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа.

**Служба прокси-сервера активации "Лаборатории Касперского"**

Необходимо отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского":*

1. Откройте список служб вашего устройства.
2. Выберите в списке службу прокси-сервера активации "Лаборатории Касперского".
3. В контекстном меню службы выберите раздел **Свойства**.

4. В окне свойства службы на закладке **Общие** в поле **Тип запуска** выберите значение **Отключена**.
5. Нажмите на кнопку **Остановить**.
6. Нажмите на кнопку **ОК**.

Служба прокси-сервера активации "Лаборатории Касперского" остановлена.

**Доверенные каналы с использованием SSL-протокола**

Для гарантированной доставки информации по доверенному каналу необходимо настроить использование SSL-соединений. В сертифицированной конфигурации программа должна использовать только доверенные каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования:*

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику **Агент администрирования**.

   Откроется окно свойств политики.
3. В окне свойств политики перейдите в раздел **Параметры программы**.
4. Выберите подраздел **Сеть**.
5. В подразделе **Сеть** выберите вложенный раздел **Подключения** и нажмите на кнопку **Параметры**.
6. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.

   Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.
7. Нажмите на кнопку **ОК**.

Подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

**Права пользователей**

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в программе. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей:*

1. В разделе **Пользователи и роли** выберите раздел **Пользователи**.
2. В поле **Полное имя** выберите пользователя или группу пользователей, которым нужно присвоить роль.

   Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.
3. Перейдите на закладку **Роли** и нажмите на кнопку **Добавить**.

   Откроется окно **Роли пользователей**. В окне отображаются созданные роли пользователей.
4. В окне **Роли пользователей** выберите роль для группы пользователей.
5. Нажмите на кнопку **ОК**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Роли** в разделе **Безопасность** окна свойств Сервера администрирования.

**Условия для статуса "Критический"**

При обнаружении на устройстве хотя бы одного вируса необходимо настроить на нем изменение статуса на *Критический*.

► *Чтобы настроить изменение статуса устройства на Критический:*

1. В разделе **Устройства** выберите **Изменить группы**.
2. Выберите группу администрирования.

   В результате откроется окно свойств группы администрирования.
3. В окне свойств перейдите в раздел **Статус устройства**.
4. В блоке **Критический** в графе **Установить статус "Критический", если:** выберите и выберитусловия **Найдено много вирусов**.
5. Нажмите на кнопку **Изменить**.
6. Для условия **Найдено много вирусов** установите значение 1.
7. Нажмите на кнопку **Сохранить**.

Изменение статуса устройства на *Критический*, при обнаружении на нем хотя бы одного вируса, настроено.

**Максимальное количество событий, хранящихся в базе данных Сервера администрирования**

Установите максимальное количество событий, хранящихся в базе данных Сервера администрирования, необходимое для проведения аудита программы. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования:*

1. Выберите Сервер администрирования, для которого нужно настроить максимальное количество событий, хранящихся на Сервере.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Сервера администрирования.
3. На закладке **Общие** выберите **Хранилище событий**.
4. В поле **Максимальное количество событий, хранящихся в базе данных** установите рекомендуемое значение, не меньше 400 000 событий.

Максимальное количество событий, хранящихся в базе данных Сервера администрирования, установлено.

По умолчанию емкость базы данных Сервера администрирования составляет 400 000 событий. Максимальная рекомендованная емкость базы данных – 15 000 000 событий. Если количество событий в базе данных достигает указанного администратором максимального значения, программа удаляет самые старые события и записывает новые.

kaspersky

**Срок хранения событий**

Для проведения аудита программы, необходимо настроить срок хранения событий в базе данных Сервера администрирования.

► *Чтобы изменить срок хранения событий:*

1. Выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Сервера администрирования.
3. В окне свойств Сервера администрирования выберите раздел **Настройка событий**.
4. Установите время хранения событий по уровню их важности:
   - На закладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На закладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На закладке **Предупреждение** выберите нужное событие установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** выберите нужное событие установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий изменен.

Срок хранения событий можно настроить также в свойствах политики Сервера администрирования.

► *Чтобы настроить срок хранения событий в свойствах политики Сервера администрирования:*

1. В разделе **Устройства** выберите раздел **Политики и профили политики**.
2. В поле **Имя политики** выберите политику, для которой нужно настроить срок хранения событий.

   Откроется окно свойств политики.
3. В окне свойств политики Сервера администрирования перейдите в раздел **Настройка событий**.
4. Установите время хранения событий, в зависимости от уровня важности событий:
   - На закладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На закладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На закладке **Предупреждение** выберите нужное событие установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** выберите нужное событие установите необходимое значение (не меньше 30 дней).
5. Нажмите на кнопку **ОК**.

Срок хранения событий изменен.

**Срок хранения ревизии изменений объектов**

Необходимо настроить срок хранения ревизии объектов, необходимый для проведения аудита программы. Рекомендуемый срок хранения ревизии изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита программы.

► *Чтобы изменить срок хранения ревизии изменения объектов:*

1. Выберите Сервер администрирования, для которого нужно настроить срок хранения изменений объектов.
2. Нажмите на кнопку **Свойства**.

   Откроется окно свойств Сервера администрирования.
3. В окне свойств Сервера администрирования на закладке **Общие** выберите раздел **Хранилище истории ревизии**.
4. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.
5. Нажмите на кнопку **Сохранить**.

Срок хранения ревизии изменения объектов изменен.

**Права доступа к возможностям шифрования**

Настройте запрет доступа к возможностям шифрования данных для всех ролей и пользователей.

► *Чтобы запретить доступ роли к возможностям шифрованию данных:*

1. Выберите Сервер администрирования.
2. Нажмите на кнопку **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Роли пользователей**.
4. Выберите роль и нажмите на кнопку **Изменить**.
5. В окне свойств роли пользователей перейдите в раздел **Права**.
6. В блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранной запрещено.

► *Чтобы запретить доступ пользователя к возможностям шифрованию данных:*

1. Выберите Сервер администрирования.
2. Нажмите на кнопку **Свойства**.
3. В окне свойств Сервера администрирования перейдите в раздел **Безопасность**.
4. Выберите пользователя и перейдите на закладку **Права**.
5. На закладке **Права** в блоке прав для программы Kaspersky Endpoint Security в области **Шифрование** установите флажок **Запретить**.

Шифрование данных для выбранного пользователя запрещено.

**Контроль целостности исполняемых модулей программы**

Запустите утилиту klscmodchk для проверки целостности исполняемых модулей программы, как описано в инструкции (см. стр. 888).

kaspersky

**Выключение объявлений, связанных с безопасностью**

Выключите объявления "Лаборатории Касперского", связанные с безопасностью, как описано в инструкции (см. стр. 1458).

# Руководство API

Руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать (см. стр. 866) задачи, которые, возможно, не хотите выполнять вручную, с помощью Консоли администрирования. Вы также можете использовать собственные сценарии, которые еще не поддерживаются в Консоли администрирования. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.
- Пользовательская разработка. Например, вы можете разработать альтернативную Консоль администрирования на основе консоли Microsoft Management Console (MMC) для своих клиентов, которая разрешает ограниченный набор действий.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

**Руководство OpenAPI https://support.kaspersky.com/help/KSC/14.2/KSCAPI/index.html**

**Примеры сценариев**

Справочное руководство по OpenAPI содержит примеры сценариев Python, перечисленные в таблице ниже. Примеры показывают, как вы можете вызывать методы OpenAPI и автоматически выполнять различные задачи по защите вашей сети, например, создавать иерархию "главный/подчиненный" (см. стр. 78), запускать задачи (см. стр. 85) в Kaspersky Security Center или назначать точки распространения (см. стр. 88). Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

► *Чтобы вызвать методы OpenAPI и запустить сценарии:*

1. Загрузите архив KlAkOAPI.tar.gz https://support.kaspersky.com/help/KSC/14.2/KSCAPI/common/KlAkOAPI-14.2.tar.gz. Этот архив включает в себя пакет KlAkOAPI и примеры (их можно скопировать из архива или справочного руководства по OpenAPI).
2. Установите пакет KlAkOAPI https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00444.html из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

*Таблица 104. Сопоставление пользовательских сценариев и примеров методов Kaspersky Security Center OpenAPI*

| Пример | Назначение примера | Сценарий |
|---|---|---|
| Log KlAkParams https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00427.html | Вы можете извлекать и обрабатывать данные с помощью структуры данных `KlAkParams`. В примере показано, как работать с этой структурой данных.<br>Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде. | Мониторинг и отчеты (см. стр. 575) |
| Создание и удаление иерархии "главный/подчиненный" https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00428.html | Вы можете добавить подчиненный Сервер администрирования и установить таким образом отношение иерархии "главный Сервер – подчиненный Сервер". Или вы можете исключить подчиненный Сервер администрирования из иерархии. | • Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования (см. стр. 984)<br>• Удаление иерархии Серверов администрирования (см. стр. 987) |
| Создайте иерархию группы со структурой на основе подразделения Active Directory. https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00429.html | Вы можете выполнить опрос подразделения Active Directory и сформировать иерархию обнаруженных групп устройств. | Создание групп администрирования (см. стр. 1124) |
| Создайте иерархию группы со структурой на основе кешированного подразделения Active Directory https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00430.html. | Вы можете сформировать иерархию групп управляемых устройств на основе ранее выполненного опроса подразделения Active Directory. Если новые устройства появляются в Active Directory после последнего опроса, они будут добавлены в группу, так как их нет в сохраненных результатах опроса. | Создание групп администрирования (см. стр. 1124) |

| Пример | Назначение примера | Сценарий |
|---|---|---|
| Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00431.html. | Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 90), а затем загрузить файл со списком сетей на свой компьютер. | Настройка точек распространения и шлюзов соединений (см. стр. 658) |
| Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00432.html | Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию. | Лицензирование управляемых программ (см. стр. 390) |
| Создайте отчет об эффективных правах пользователей https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00433.htm | Вы можете создать разные отчеты https://stage.help.kaspersky.com/KSC/14.2/KSCAPI/a00032.html. Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли.<br>Вы можете загрузить отчет в формате HTML, PDF или Excel. | Генерация и просмотр отчета (см. стр. 1372) |
| Запустить задачу для устройства https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00434.html. | Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 90), а затем запустить необходимую задачу. | Запустите задачу вручную (см. стр. 1112). |
| Создание IP-подсетей на основе сайта и служб Active Directory https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00435.html | Вы можете создать IP-подсеть на основе используемого подразделения Active Directory.<br>В примере запускается опрос указанного диапазона IP-адресов и удаляются обнаруженные подсети, чтобы избежать их конфликта с новой подсетью. Поэтому не запускайте такой пример в сети, где важно сохранить подсети.<br>После опроса пример кода обращается к Active Directory, проверяет каждое устройство в нем и создает IP-подсеть. Для этого в примере используются маски и IP-адреса всех устройств. | Настройка защиты сети (см. стр. 400). |

| Пример | Назначение примера | Сценарий |
| --- | --- | --- |
| Регистрация точек распространения для устройств в группе https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00436.html | Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений"). | Обновление баз и программ "Лаборатории Касперского" (см. стр. 1234) |
| Перечисление всех групп https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00437.html | Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее:<br>• Получить идентификатор корневой группы "Управляемые устройства".<br>• Переместить по иерархии групп.<br>• Получить полную развернутую иерархию групп с их именами и вложенностью. | Настройка Сервера администрирования (см. стр. 980) |
| Перечисление задач, запрос статистики задач и запуск задач https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00438.html | Вы можете ознакомиться со следующей информацией:<br>• Историей выполнения задачи.<br>• Текущим статусом задачи.<br>• Количеством задач в разных статусах.<br>Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики. | Наблюдение за ходом выполнения задачи (см. стр. 420). |
| Создание и запуск задачи https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00439.html | Вы можете создать задачу. Укажите в примере следующие параметры задачи:<br>• Тип.<br>• Способ запуска.<br>• Имя.<br>• Группа устройств, для которой будет использоваться задача.<br>По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00030.html. | Создание задачи (см. стр. 413). |
| Перечисление лицензионных ключей https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00440.html. | Вы можете получить список всех активных лицензионных ключей для программ "Лаборатории Касперского", установленных на управляемых | Просмотр информации об используемы |

| Пример | Назначение примера | Сценарий |
|---|---|---|
| | устройствах Сервера администрирования. Список содержит подробные сведения https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00117.html о каждом лицензионном ключе, такие как имя, тип или срок действия. | х лицензионны х ключах (см. стр. 392). |
| Создание и поиск внутреннего пользователя https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00441.html | Вы можете создать учетную запись для дальнейшей работы. | Выбор учетной записи для запуска Сервера администрир ования (см. стр. 249). |
| Создание пользовательской категории https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00442.html | Вы можете создать категорию программ с требуемыми параметрами https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00450.html. | Создание пополняемой вручную категории программ (см. стр. 1342) |
| Перечисление пользователей с помощью SrvView https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00443.html | Вы можете использовать класс SrvView https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00582.html для запроса подробной информации https://support.kaspersky.com/help/KSC/14.2/KSCAPI/a00154.html с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример. | Управление учетными записями пользователе й (см. стр. 764). |

**Программы, взаимодействующие с Kaspersky Security Center через OpenAPI**

Некоторые программы взаимодействуют с Kaspersky Security Center через OpenAPI. К таким программам относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательская клиентская программа, разработанная вами на основе OpenAPI.

Программы, взаимодействующие с Kaspersky Security Center через OpenAPI, подключаются к Серверу администрирования. Если вы настроили список разрешенных IP-адресов (см. стр. 678) для подключения к Серверу администрирования, добавьте IP-адреса устройств, на которых установлены программы, использующие Kaspersky Security Center OpenAPI. Чтобы узнать, работает ли используемая вами программа с OpenAPI, обратитесь к справке этой программы.

kaspersky

# Лучшие практики для поставщиков услуг

В этой справке вы можете найти информацию о настройке и использовании Kaspersky Security Center https://help.kaspersky.com/KSC/14.2/ru-RU/180118.htm.

Документ содержит рекомендации по развертыванию, настройке и использованию программы, а также способы решения типичных проблем, возникающих при работе программы.

kaspersky

# Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center https://help.kaspersky.com/KSC/14.2/ru-RU/180118.htm.

kaspersky

# Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

## В этом разделе



## Способы получения технической поддержки

Если вы не нашли решения вашего вопроса в документации Kaspersky Security Center или других источниках информации о программе, обратитесь в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center.

"Лаборатория Касперского" предоставляет поддержку Kaspersky Security Center в течение ее жизненного цикла (см. страницу жизненного цикла программ (https://support.kaspersky.com/corporate/lifecycle)). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки (https://support.kaspersky.com/support/rules/ru_ru).

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить веб-сайт Службы технической поддержки (https://support.kaspersky.ru/b2c);
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount portal (https://companyaccount.kaspersky.com).

## Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/faq/companyaccount_help).

kaspersky

# Глоссарий

## A

### Активный ключ

Ключ, используемый в текущий момент для работы программы.

### Дополнительный лицензионный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

### Консоль администрирования

Компонент Kaspersky Security Center на базе Windows (далее также Консоль администрирования на основе MMC). Этот компонент предоставляет пользовательский интерфейс к административным службам Сервера администрирования и Агента администрирования.

### Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

### Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Сервер администрирования может также управлять этими программами.

### сертификат Сервера администрирования;

Сертификат, который Сервер администрирования использует для следующих целей:

- Аутентификация Сервера администрирования при подключении к Консоли администрирования на основе MMC или Kaspersky Security Center 14.2 Web Console.
- безопасное взаимодействие Сервера администрирования с Агентами администрирования на управляемых устройствах;
- аутентификация Серверов администрирования при подключении главного Сервера администрирования к подчиненному Серверу администрирования.

Сертификат создается автоматически при установке Сервера администрирования и затем хранится на Сервере администрирования.

### Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые программы "Лаборатории Касперского".

## Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования;

## Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

## Рабочее место администратора

Устройство, на котором установлена Консоль администрирования или которое вы используете для работы с Kaspersky Security Center 14.2 Web Console. Этот компонент, предоставляет интерфейс управления Kaspersky Security Center.

С рабочего места администратор управляет серверной частью Kaspersky Security Center. Используя рабочее место администратора, администратор выстраивает систему централизованной защиты сети организации, сформированной на базе программ "Лаборатории Касперского".

## Инстанс Amazon EC2

Виртуальная машина, созданная на основе образа AMI с использованием Amazon Web Services.

## Amazon Machine Image (AMI)

Шаблон с необходимой для запуска виртуальной машины конфигурацией программного обеспечения. На основе одного образа AMI можно создать несколько инстансов.

## Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать в проверяемых объектах вредоносный код. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

## Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

### Магазин приложений

Компонент программы Kaspersky Security Center. Магазин приложений используется для установки приложений на Android-устройства пользователей. В магазине приложений можно публиковать apk-файлы приложений и ссылки на приложения в Google Play.

### Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

### Доступное обновление

Пакет обновлений модулей программы "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

### AWS Application Program Interface (AWS API)

Программный интерфейс приложения платформы AWS, который используется программой Kaspersky Security Center. Средствами AWS API проводятся, в частности, опрос облачных сегментов и установка Агента администрирования на инстансы.

### Ключ доступа AWS IAM

Комбинация, состоящая из ID ключа (вида "AKIAIOSFODNN7EXAMPLE") и секретного ключа (вида "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Пара принадлежит IAM-пользователю и используется для получения доступа к сервисам AWS.

### Консоль управления AWS

Веб-интерфейс для просмотра и управления ресурсами в AWS. Консоль управления AWS доступна в интернете на странице https://aws.amazon.com/ru/console/.

## B

### Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

### Широковещательный домен

Логический участок компьютерной сети, в котором все узлы могут передавать данные друг другу с помощью широковещательного канала на уровне сетевой модели OSI (Open Systems Interconnection Basic Reference Model).

kaspersky

# C

## Централизованное управление программой

Удаленное управление программой при помощи служб администрирования, предоставляемых Kaspersky Security Center.

## Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной защиты организации-клиента.

## Облачное окружение

Виртуальные машины или другие виртуальные ресурсы на базе облачной платформы, объединенные в сети.

## Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

## Шлюз соединения

*Шлюз соединения* – это Агент администрирования, работающий в особом режиме. Шлюз соединения принимает соединения от других Агентов администрирования и туннелирует их к Серверу администрирования через собственное соединение с Сервером. В отличие от обычного Агента администрирования, шлюз соединения ожидает соединений от Сервера администрирования, а не устанавливает соединения с Сервером администрирования.

# D

## Демилитаризованная зона (DMZ)

Демилитаризованная зона – это сегмент локальной сети, в которой находятся серверы, отвечающие на запросы из глобальной сети. В целях обеспечения безопасности локальной сети организации доступ в локальную сеть из демилитаризованной зоны ограничен и защищен сетевым экраном.

## Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

## Непосредственное управление программой

Управление программой через локальный интерфейс.

## Точка распространения

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в составе группы администрирования и / или широковещательного домена. Точки распространения предназначены для

уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Точки распространения могут быть назначены автоматически Сервером администрирования или вручную администратором. Точка распространения ранее называлась агентом обновлений.

# E

## EAS-устройство

Мобильное устройство, которое подключается к Серверу администрирования по протоколу Exchange ActiveSync. По протоколу Exchange ActiveSync могут подключаться и управляться устройства с операционными системами iOS, Android, Windows Phone®.

## Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center.

## Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют следующие уровни важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

## Сервер мобильных устройств Exchange ActiveSync

Компонент Kaspersky Security Center, который позволяет подключать мобильные устройства Exchange ActiveSync к Серверу администрирования.

# F

## Принудительная установка

Метод удаленной установки программ "Лаборатории Касперского", который позволяет провести удаленную установку программного обеспечения на конкретные клиентские устройства. Для успешного выполнения задачи методом принудительной установки учетная запись для запуска задачи должна обладать правами на удаленный запуск программ на клиентских устройствах. Данный метод рекомендуется для установки программ на устройства, работающие под управлением операционных систем Microsoft Windows, в которых поддерживается такая возможность.

kaspersky

# G

## Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

# H

## Домашний Сервер администрирования

Домашний Сервер администрирования – это Сервер администрирования, который был задан при установке Агента администрирования. Домашний Сервер администрирования может использоваться в параметрах профилей подключения Агента администрирования.

## HTTPS

Безопасный протокол передачи данных между браузером и веб-сервером с использованием шифрования. HTTPS используется для доступа к закрытой информации, такой как корпоративные или финансовые данные.

# I

## IAM-роль

Совокупность прав для выполнения запросов к сервисам AWS. IAM-роли не связаны ни с каким конкретным пользователем или группой и обеспечивают права доступа без использования ключей доступа AWS IAM. IAM-роль можно присвоить пользователям IAM, инстансам EC2, приложениям или сервисам AWS.

## IAM-пользователь

Пользователь сервисов AWS. IAM-пользователь может обладать правами на опрос облачного сегмента.

## Identity and Access Management (IAM)

Сервис AWS, который позволяет управлять доступом пользователей к другим сервисам и ресурсам AWS.

## Несовместимая программа

Антивирусная программа стороннего производителя или программа "Лаборатории Касперского", не поддерживающая управление через Kaspersky Security Center.

## Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

### Внутренние пользователи

Учетные записи внутренних пользователей используются для работы с виртуальными Серверами администрирования. В программе Kaspersky Security Center внутренние пользователи обладают правами реальных пользователей.

Учетные записи внутренних пользователей создаются и используются только внутри Kaspersky Security Center. Сведения о внутренних пользователях не передаются операционной системе. Аутентификацию внутренних пользователей осуществляет Kaspersky Security Center.

### iOS MDM-устройство

Мобильное устройство, которое подключается к Серверу iOS MDM по протоколу iOS MDM. По протоколу iOS MDM могут подключаться и управляться устройства с операционной системой iOS.

### iOS MDM-профиль

Набор параметров подключения мобильных устройств iOS к Серверу администрирования. Пользователь устанавливает iOS MDM-профиль на мобильное устройство, после чего это мобильное устройство подключается к Серверу администрирования.

### Сервер iOS MDM

Компонент Kaspersky Security Center, который устанавливается на клиентское устройство и позволяет подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью сервиса Apple Push Notifications (APNs).

## J

### JavaScript

Язык программирования, расширяющий возможности веб-страниц. Веб-страницы, созданные с использованием JavaScript, способны выполнять дополнительные действия (например, изменять вид элементов интерфейса или открывать дополнительные окна) без обновления веб-страницы данными с веб-сервера. Чтобы просматривать веб-страницы, созданные с использованием JavaScript, в параметрах браузера надо включить поддержку JavaScript.

## K

### Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – это решение, которое предоставляет пользователям устройств, с установленными программами "Лаборатории Касперского", доступ к базам данных Kaspersky Security Network и другим статистическим данным, без отправки данных со своих устройств в Kaspersky Security Network. Kaspersky Private Security Network предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

- Устройства не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

kaspersky

## Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

## Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

## Kaspersky Security Center System Health Validator (SHV)

Компонент программы Kaspersky Security Center, предназначенный для проверки работоспособности операционной системы при совместной работе программы Kaspersky Security Center с Microsoft NAP.

## Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается в составе Сервера администрирования. Веб-сервер предназначен для передачи по сети автономных инсталляционных пакетов, iOS MDM-профилей, а также файлов из папки общего доступа.

## Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

## Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

## KES-устройство

Мобильное устройство, которое подключается к Серверу администрирования и управляется с помощью мобильного приложения Kaspersky Endpoint Security для Android.

## Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии.

kaspersky

# L

## Срок действия лицензии

Период, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

## Группа лицензионных программ

Группа программ, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

## Локальная установка

Установка программы безопасности на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива программы безопасности или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

## Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском компьютере.

# M

## Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

## Плагин управления

Специализированный компонент, предоставляющий интерфейс для управления работой программы через Консоль администрирования. Он входит в состав всех программ "Лаборатории Касперского", управление которыми может осуществляться при помощи Kaspersky Security Center.

## Ручная установка

Установка программы безопасности на устройство сети организации из дистрибутива программы безопасности. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

## Сервер мобильных устройств

Компонент Kaspersky Security Center, который предоставляет доступ к мобильным устройствам и позволяет управлять ими через Консоль администрирования.

kaspersky

# N

## Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft® Windows®. Для программ "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.

## Антивирусная безопасность сети

Комплекс технических и организационных мер, снижающих вероятность проникновения на устройства сети организации вирусов и спама, предотвращающих сетевые атаки, фишинг и другие угрозы. Антивирусная безопасность сети повышается при использовании программ безопасности и служб, а также при наличии и соблюдении политики информационной безопасности в организации.

## Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных программ безопасности, использование лицензионных ключей, количество и виды обнаруженных угроз.

# P

## Уровень важности патча

Характеристика патча. Для патчей сторонних производителей или Microsoft существует пять уровней важности:

- Предельный.
- Высокий.
- Средний.
- Низкий.
- Неизвестно.

Уровень важности патча стороннего производителя или Microsoft определяется наиболее неблагоприятным уровнем критичности уязвимости, которую закрывает патч.

## Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать множество политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

## Профиль

Набор параметров поведения мобильных устройств Exchange при подключении к серверу Microsoft Exchange.

kaspersky

### Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

### Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

### Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

## R

### Удаленная установка

Установка программ "Лаборатории Касперского" при помощи инструментов, предоставляемых программой Kaspersky Security Center.

### Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

### Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования;

### Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами (см. стр. 1492).

kaspersky

# S

## Администратор поставщика услуг

Сотрудник организации-поставщика услуг антивирусной защиты. Выполняет работы по инсталляции, эксплуатации систем антивирусной защиты, созданных на основе решений "Лаборатории Касперского", а также осуществляет техническую поддержку клиентов.

## Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

## SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

# T

## Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

## Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

## Параметры задачи

Параметры работы программы, специфичные для каждого типа задачи.

# U

## Устройство с защитой на уровне UEFI

Устройство со встроенным на уровне BIOS программным обеспечением Антивирус Касперского для UEFI. Встроенная защита обеспечивает безопасность устройства еще с начала запуска системы, в то время как защита устройств, не имеющих встроенного ПО, начинает действовать только после запуска программы безопасности.

## Обновление

Процедура замены или добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

# V

## Виртуальный Сервер администрирования

Компонент программы Kaspersky Security Center, предназначенный для управления системой защиты сети организации-клиента.

Виртуальный Сервер администрирования является частным случаем подчиненного Сервера администрирования и, по сравнению с физическим Сервером администрирования, имеет следующие основные ограничения:

- Виртуальный Сервер администрирования может функционировать только в составе главного Сервера администрирования.
- Виртуальный Сервер администрирования при работе использует основную базу данных главного Сервера администрирования. Задачи резервного копирования и восстановления данных, а также задачи проверки и загрузки обновлений, не поддерживаются на виртуальном Сервере администрирования.
- Для виртуального Сервера не поддерживается создание подчиненных Серверов администрирования (в том числе и виртуальных).

## Порог вирусной активности

Максимально допустимое количество событий заданного типа в течение ограниченного времени, превышение которого будет считаться повышением вирусной активности и возникновением угрозы вирусной атаки. Данная характеристика имеет большое значение в периоды вирусных эпидемий и позволяет администратору своевременно реагировать на возникающие угрозы вирусных атак.

## Вирусная атака

Ряд целенаправленных попыток заразить устройство вирусом.

## Уязвимость

Недостаток в операционной системе или программе, который может быть использован производителями вредоносного программного обеспечения для проникновения в операционную систему или программу и нарушения ее целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вирусы могут вызывать сбои в работе как самой операционной системы, так и установленных программ.

# W

## Windows Server Update Services (WSUS)

Программа, которая используется для распространения обновлений программ Microsoft на устройствах пользователей в сети организации.

kaspersky

# Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

kaspersky

# Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft, MultiPoint, MS-DOS, PowerShell, PowerPoint, SQL Server, OneNote, OutLook, Tahoma, Win32, Windows, Windows PowerShell, Windows Server, Windows Phone, Windows Vista, Windows Azure – являются товарными знаками группы компаний Microsoft.

Adobe является зарегистрированным товарным знаком или товарным знаком компании Adobe в США и (или) других странах.

AirPlay, AirDrop, AirPrint, App Store, Apple, AppleScript, FaceTime, FileVault, iBook, iBooks, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – товарные знаки Apple Inc.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Cisco, Cisco Systems, IOS – зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и / или ее аффилированных компаний.

Citrix, XenServer – товарные знаки Citrix Systems, Inc. и / или дочерних компаний, зарегистрированные в патентном офисе США и других стран.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Android, Chrome, Dalvik, Google, Google Play, Google Карты, Google Analytics, Hangouts, YouTube – товарные знаки Google LLC.

Firefox – товарный знак Mozilla Foundation, зарегистрированный в США и других странах.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

JavaScript, Python, TouchDown, Oracle и Java – зарегистрированные товарные знаки Oracle Corporation и / или ее аффилированных компаний.

QRadar, IBM – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Intel, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

CentOS, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

Novell – товарный знак Novell Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

SPL, Splunk – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

VMware, VMware vSphere – товарный знак VMware, Inc. или зарегистрированный в США или других юрисдикциях товарный знак VMware, Inc.

kaspersky

# Известные ошибки и ограничения

Kaspersky Security Center 14.2 Web Console имеет ряд ограничений, не критичных для работы программы:

- Если правило Контроля программ основано на категории программ, в которую входят программы, обнаруженные на устройствах с операционной системой Linux, правило не работает. При выборе программ из реестра программ, для их добавления в категорию программ убедитесь, что вы выбираете программы, обнаруженные на устройствах с операционной системой Windows.
- Если на устройстве с операционной системной Linux обнаружена программа из раздела **Реестр программ**, в свойствах программы отсутствует информация о связанных с ней исполняемых файлах.
- Если вы устанавливаете Агент администрирования на устройство под управлением операционной системы ALT Linux с помощью задачи удаленной установки и запускаете эту задачу под учетной записью с правами, отличными от root, задача не будет выполнена. Запустите задачу удаленной установки под учетной записью root или создайте и используйте автономный инсталляционный пакет Агента администрирования для локальной установки программы.
- Если отчет содержит более 20 записей (в этом случае записи отображаются на нескольких страницах) и вы установили флажок **Выбрать все**, Web Console выбирает только те записи, которые отображаются на текущей странице.
- После завершения локальной задачи *Поиск IOC*, состояние задачи отображается как *Запланировано*.
- Клиентские устройства могут быть не найдены после запуска опроса сети Windows.
- В политике Kaspersky Endpoint Security для Windows при выборе и применении категории программы при настройке функции Контроля программ категория применяется, но не отображается как выбранная после сохранения и повторного открытия политики.
- После отключения службы прокси-сервера KSN, устройства в группе Управляемые устройства меняют свой статус на *Критический*, а устройства в подгруппах отображаются со статусом *ОК*.
- Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, используйте тот же регистр при указании DNS-имени устройства в правилах перемещения устройств и правилах автоматического назначения тегов. Иначе правила не будут работать.
- В мастере **Добавить подчиненный Сервер администрирования**, если указать учетную запись с включенной двухэтапной проверкой для аутентификации на будущем подчиненном Сервере, мастер завершает работу с ошибкой. Чтобы решить эту проблему, укажите учетную запись, для которой выключена двухэтапная проверка, или создайте иерархию из будущего подчиненного Сервера.
- При входе в Kaspersky Security Center 14.2 Web Console, если вы используете доменную аутентификацию и указываете виртуальный Сервер администрирования для подключения, затем выходите из программы и пытаетесь войти на главный Сервер администрирования, Kaspersky Security Center 14.2 Web Console все равно подключается к виртуальному Серверу администрирования. Чтобы подключиться к главному Серверу администрирования, повторно откройте браузер.
- Некорректный статус локальной задачи может отображаться в списке задач в свойствах устройства.
- Быстрый/полный опрос сети Windows возвращает пустой результат.
- Если вы устанавливаете Kaspersky Security Center 14.2 Web Console с Identity and Access Manager, а затем меняете Сервер администрирования Kaspersky Security Center 14.2 Web Console, компонент Identity and Access Manager не получает информацию о новом Сервере администрирования.

- Если вы открываете Kaspersky Security Center 14.2 Web Console в разных браузерах и загружаете файл сертификата Сервера администрирования в окне свойств Сервера администрирования, загруженные файлы имеют разные имена.
- Ошибка возникает при попытке восстановить объект из хранилища **Резервное хранилище** (**Операции** → **Хранилища** → **Резервное хранилище**) или при отправке объекта в "Лабораторию Касперского".
- Управляемое устройство, имеющее более одного сетевого адаптера, отправляет Серверу администрирования информацию о MAC-адресе сетевого адаптера, отличного от того, который используется для подключения к Серверу администрирования.
- Если вы устанавливаете Kaspersky Security Center 14.2 Web Console с Identity and Access Manager, а затем меняете Сервер администрирования Kaspersky Security Center 14.2 Web Console, компонент Identity and Access Manager не получает информацию о новом Сервере администрирования.

kaspersky

# АО «Лаборатория Касперского»

"Лаборатория Касперского" – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году "Лаборатория Касперского" вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг IDC Worldwide Endpoint Security Revenue by Vendor). В России, по данным IDC, "Лаборатория Касперского" – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей (IDC Endpoint Tracker 2014).

"Лаборатория Касперского" основана в России в 1997 году. Сегодня "Лаборатория Касперского" – это международная группа компаний с 38 офисами в 33 странах мира. В компании работает более 3000 квалифицированных специалистов.

**Продукты**. Продукты "Лаборатории Касперского" защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты "Лаборатории Касперского" сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики "Лаборатории Касперского" работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами "Лаборатории Касперского".

**Технологии**. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно "Лабораторией Касперского". Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

**Достижения**. За годы борьбы с компьютерными угрозами "Лаборатория Касперского" завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, "Лаборатория Касперского" стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда "Лаборатории Касперского" – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

kaspersky

| | |
|---|---|
| Сайт "Лаборатории Касперского": | https://www.kaspersky.ru |
| Вирусная энциклопедия: | https://securelist.ru/ |
| Kaspersky VirusDesk: | https://virusdesk.kaspersky.ru (для проверки подозрительных файлов и сайтов) |
| Сообщество пользователей "Лаборатории Касперского": | https://community.kaspersky.com |

kaspersky

# Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

*Таблица 105. Соответствие терминов*

| Термин в документации | Термин в требованиях ФСТЭК |
|---|---|
| программа | продукт, объект оценки, программное изделие |
| виртуальная инфраструктура VMware | среда функционирования |
| файл виртуальной машины | объект воздействия |
| вирус, программа, представляющая угрозу, вредоносная программа | КВ, компьютерный вирус |
| антивирусные базы, базы программы | базы данных признаков компьютерных вирусов (БД ПКВ) |
| САВЗ | средство антивирусной защиты |
| антивирусная проверка | поиск вирусов |
| события | данные аудита |
| администратор | администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь |