kaspersky

Kaspersky Security Center (для Linux)

Подготовительные процедуры и руководство по эксплуатации

Версия программы: 15.0.0.12912

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: 05.09.2023

Обозначение документа: 643.46856491.00069-10 90 01

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

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

kaspersky

Содержание

kaspersky

Об этом документе

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

Подготовительные процедуры изложены в разделах "Начало работы", "Установка", "Мастер первоначальной настройки" 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, 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 https://support.kaspersky.com/KSCLinux/15/ru-RU 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. 611).

kaspersky

Требования

Этот раздел содержит аппаратные и программные требования для установки и работы программы, а также указания по эксплуатации и требования к среде.

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. Должна быть обеспечена синхронизация по времени между компонентами программы, а также между программой и средой ее функционирования.
9. Персонал, ответственный за функционирование программы, должен обеспечивать надлежащее функционирование программы, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между программой и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование программы должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности программы.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности программы.

14. Управление атрибутами безопасности, связанными с доступом к функциям и данным программы, должно предоставляться только уполномоченным ролям (администраторам программы и информационной системы).
15. 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.
16. 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.
17. Запрещается использовать прокси-серверы с протоколом socks5.

Аппаратные и программные требования

Требования к Серверу администрирования

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.

Поддерживаются следующие операционные системы:

- Debian GNU/Linux 10.x (Buster) 64-разрядная.
- Debian GNU/Linux 11.x (Bullseye) 64-разрядная.
- Debian GNU/Linux 12 (Bookworm) 64-разрядная.
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- CentOS 7.x 64-разрядная.
- CentOS Stream 9 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.
- Astra Linux Special Edition РУСБ.10015-01 (обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (обновление 1.7) 64-разрядная.

- Astra Linux Common Edition (обновление 2.12) 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- Альт Сервер 10 64-разрядная.
- Альт Сервер 9.2 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.
- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Oracle Linux 9 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware vSphere 8.0.
- VMware Workstation 16 Pro.
- VMware Workstation 17 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.
- Oracle VM VirtualBox 7.x.
- Виртуальная машина на основе Kernel (все операционные системы Linux, поддерживаемые Сервером администрирования).

Поддерживаются следующие серверы баз данных (могут быть установлены на другой машине):

- MySQL 5.7 Community 32-разрядная/64-разрядная.
- MySQL 8.0 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 Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- PostgreSQL 15.x 64-разрядная.
- Postgres Pro 13.x (все редакции) 64-разрядная.
- Postgres Pro 14.x (все редакции) 64-разрядная.
- Postgres Pro 15.x (все редакции) 64-разрядная.
- Platform V Pangolin 5.4.0 64-разрядная.

Требования к Web Console

Сервер Kaspersky Security Center Web Console

Минимальные аппаратные требования:

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

Одна из следующих операционных систем (только 64-разрядные версии):

- Debian GNU/Linux 10.x (Buster).
- Debian GNU/Linux 11.x (Bullseye).
- Debian GNU/Linux 12 (Bookworm).
- Ubuntu Server 18.04 LTS (Bionic Beaver).
- Ubuntu Server 20.04 LTS (Focal Fossa).
- Ubuntu Server 22.04 LTS (Jammy Jellyfish).
- CentOS Stream 9.
- 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 РУСБ.10015-01 (обновление 1.6).
- Astra Linux Special Edition РУСБ.10015-01 (обновление 1.7).
- Astra Linux Common Edition (обновление 2.12).
- Альт СП Сервер 10.

- Альт Сервер 10.
- Альт Сервер 9.2.
- 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.
- РОСА "КОБАЛЬТ" 7.9.
- Виртуальная машина на основе Kernel (все операционные системы Linux, поддерживаемые Сервером Kaspersky Security Center Web Console).

Клиентские устройства

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

Требования к аппаратному и программному обеспечению устройства совпадают с требованиями к браузеру, который используется для работы с Kaspersky Security Center Web Console.

Браузеры:

- Google™ Chrome™ 100.0.4896.88 или более поздняя версия (официальная сборка).
- Microsoft® Edge 100 или более поздняя версия.
- Safari® 15 для macOS®.
- Яндекс Браузер 23.5.0.2271 и выше.
- Mozilla Firefox Extended Support Release 102.0 или более поздняя версия.

Требования к Агенту 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: 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 7 Standard Service Pack 1 32-разрядная/64-разрядная.

- Microsoft Windows Embedded 8.1 Industry Pro 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/64-разрядная.
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-разрядная/64-разрядная.
- 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 1909 32-разрядная/64-разрядная.
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32-разрядная/64-разрядная.
- Microsoft Windows 10 IoT Enterprise version 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 3 и выше 32-разрядная.
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная.
- Windows Small Business Server 2011 Essentials 64-разрядная.
- Windows MultiPoint Server 2011 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.
- Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная.
- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная.

- Debian GNU/Linux 12 (Bookworm) 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 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- CentOS 7.x 64-разрядная.
- CentOS Stream 9 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 Service Pack 3 ARM 64-разрядная.
- openSUSE 15 64-разрядная.
- EulerOS 2.0 SP8 ARM.
- Astra Linux Special Edition РУСБ.10015-01 (обновление 1.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (обновление 1.7) 64-разрядная.
- Astra Linux Common Edition (обновление 2.12) 64-разрядная.
- Astra Linux Special Edition РУСБ.10152-02 (обновление 4.7) ARM 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Альт Сервер 10 64-разрядная.
- Альт Сервер 9.2 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 (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.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 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.
- macOS Big Sur (11.x).
- macOS Monterey (12.x).
- macOS Ventura (13.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 vSphere 8.0.
- VMware Workstation 16 Pro.
- VMware Workstation 17 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.
- Oracle VM VirtualBox 7.x.
- Виртуальная машина на основе Kernel (все операционные системы Linux, поддерживаемые Агентом администрирования).

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 MultiPoint Server 2011 убедитесь, что у установлено обновление для Windows 7 (KB3063858) https://www.microsoft.com/ru-ru/download/details.aspx?id=47442.

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно (см. стр. 209)

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 для Linux.

Агент администрирования для macOS поставляется вместе с программой безопасности "Лаборатории Касперского" для этой операционной системы.

Неподдерживаемые операционные системы и платформы

- Неподдерживаемые операционные системы и платформы. Сервер администрирования (см. стр. 27)
- Неподдерживаемые операционные системы и платформы. Сервер Kaspersky Security Center Web Console (см. стр. 30)
- Неподдерживаемые операционные системы и платформы. Агент администрирования (см. стр. 31)

Неподдерживаемые операционные системы и платформы. Сервер администрирования

Сервер администрирования несовместим со следующими операционными системами:

- Debian GNU/Linux 7.x (до 7.8) 32-разрядная/64-разрядная.
- Debian GNU/Linux 8.x (Jessie) 32-разрядная/64-разрядная.
- Debian GNU/Linux 9.x (Stretch) 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 Server 18.04 LTS (Bionic Beaver) 32-разрядная.
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-разрядная.
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-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 1.5 64-разрядная.
- Astra Linux Special Edition РУСБ.10152-02 (обновление 4.7) ARM 64-разрядная.
- Альт Рабочая станция 9.2 32-разрядная/64-разрядная.
- Альт Рабочая станция 10 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.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 "ХРОМ" 12 64-разрядная.
- Лотос (версия ядра Linux 4.19.50, DE: MATE) 64-разрядная.

Сервер баз данных:

- 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) 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.
- 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 Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.

Следующие платформы виртуализации не поддерживаются:

- VMware vSphere 4.1.
- VMware vSphere 5.0.
- VMware vSphere 5.1.
- VMware vSphere 5.5.
- VMware vSphere 6.
- 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 SQL Server 2008 R2 Service Pack 1 и выше 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.

Неподдерживаемые операционные системы и платформы. Сервер Kaspersky Security Center Web Console

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

- Debian GNU/Linux 7.x (до 7.8) 32-разрядная/64-разрядная.
- Debian GNU/Linux 8.x (Jessie) 32-разрядная/64-разрядная.
- Debian GNU/Linux 9.x (Stretch) 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 Server 20.04.04 LTS (Focal Fossa) ARM 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 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 1.5 64-разрядная.
- Astra Linux Special Edition РУСБ.10152-02 (обновление 4.7) ARM 64-разрядная.
- Альт Рабочая станция 9.2 32-разрядная/64-разрядная.
- Альт Рабочая станция 10 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.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 "ХРОМ" 12 64-разрядная.
- Лотос (версия ядра Linux 4.19.50, DE: MATE) 64-разрядная.

Неподдерживаемые операционные системы и платформы. Агент администрирования

Следующие операционные системы не поддерживаются:

- Microsoft Windows Embedded POSReady 7 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 Enterprise 32-разрядная/64-разрядная.
- Microsoft Windows Embedded 8.1 Industry Update 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 и выше 32-разрядная/64-разрядная.
- Microsoft Windows Vista Enterprise Service Pack 2 и выше 32-разрядная/64-разрядная.
- Microsoft Windows Vista Ultimate Service Pack 2 и выше 32-разрядная/64-разрядная.
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная.
- Microsoft Windows XP Home Service Pack 3 и выше 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 2003 R2 Standard 32-разрядная.
- Windows Small Business Server 2003 R2 Premium 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.
- Microsoft Windows Home Server 2011 64-разрядная.
- Windows MultiPoint Server 2010 Standard 64-разрядная.
- Windows MultiPoint Server 2010 Premium 64-разрядная.
- Windows MultiPoint Server 2012 Standard/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 with Service Pack 1 32-разрядная/64-разрядная.
- Windows Server 2008 Service Pack 1 Server Core 32-разрядная/64-разрядная.
- Windows Server 2008 Standard with 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.
- 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 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 Server 20.04.04 LTS (Focal Fossa) ARM 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.
- SUSE Linux Enterprise Desktop 12 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Desktop 15 (все пакеты обновлений) 64-разрядная.
- Astra Linux Special Edition 1.5 64-разрядная.
- Astra Linux Special Edition РУСБ.10265-01 (обновление 8.1) Elbrus.
- Astra Linux Special Edition РУСБ.10015-16 (обновление 8.1) Elbrus.
- Pardus OS 19.1 64-разрядная.
- Linux Mint 19.x 32-разрядная.
- Лотос (версия ядра Linux 4.19.50, DE: MATE) 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.

Следующие платформы виртуализации не поддерживаются:

- VMware vSphere 4.1.
- VMware vSphere 5.0.
- VMware vSphere 5.1.
- VMware vSphere 5.5.
- VMware vSphere 6.
- 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 SQL Server 2008 R2 Service Pack 1 и выше 64-разрядная.
- Citrix XenServer 6.0.
- Citrix XenServer 6.1.
- Citrix XenServer 6.2.
- Citrix XenServer 6.5.
- Citrix XenServer 7.

kaspersky

О Kaspersky Security Center

В этом разделе представлена информация о назначении, ключевых возможностях и составе Kaspersky Security Center, аппаратные и программные требования для установки и работы Kaspersky Security Center, а также указания по эксплуатации и требования к среде.

Программа Kaspersky Security Center предназначена для развертывания и управления защитой устройств с операционной системой Linux® с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux.

Программа Kaspersky Security Center является средством антивирусной защиты типа "А" и позволяет вам устанавливать программы безопасности "Лаборатории Касперского" на устройства в корпоративной сети, удаленно запускать задачи проверки и обновления, а также управлять политиками безопасности управляемых программ. Как администратор, вы можете использовать панель мониторинга, где показано актуальное состояние корпоративных устройств, отображаются подробные отчеты и детальные параметры политик.

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.

По сравнению с Kaspersky Security Center на базе Windows®, Kaspersky Security Center на базе Linux® имеет другой набор функций (см. стр. 38).

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

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".
- Выполнять удаленную установку программ "Лаборатории Касперского" и других программ сторонних производителей.
- 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".

- 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.

В этом разделе

Список поддерживаемых программ "Лаборатории Касперского"

Kaspersky Security Center поддерживает удаленную установку и управление следующими программами "Лаборатории Касперского":

- Kaspersky Endpoint Security для Linux
- Kaspersky Endpoint Security для Linux Elbrus Edition
- Kaspersky Endpoint Security для Linux ARM Edition
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent (поддерживается в сценарии с использованием Kaspersky Anti Targeted Attack/EDR https://support.kaspersky.com/KATA/5.0/ru-RU/192894.htm)
- Kaspersky Security для виртуальных сред Легкий агент
- Kaspersky Embedded Systems Security для Windows
- Kaspersky Embedded Systems Security для Linux

Эти программы позволяют защитить как рабочие станции, так и файловые серверы. Подробнее о версиях программ и решений см. на странице "Жизненный цикл программ" https://support.kaspersky.com/corporate/lifecycle.

Поддерживается Kaspersky Endpoint Security для Windows. Известные ошибки и ограничения

В Kaspersky Endpoint Security для Windows версии 12.0 добавлена ограниченная поддержка Kaspersky Security Center. Следующие ограничения являются наиболее критичными:

- Компонент Адаптивный контроль аномалий не поддерживается. Kaspersky Security Center не поддерживает правила Адаптивного контроля аномалий.
- Компоненты Kaspersky Sandbox не поддерживаются.

kaspersky

О совместимости Сервера администрирования и Kaspersky Security Center 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 Web Console поддерживает Сервер администрирования Kaspersky Security Center следующих версий: 14.2, 14 и 13.2.
- Сервер администрирования Kaspersky Security Center 15 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. Этот документ содержит информацию о Kaspersky Security Center для Linux. Для получения подробной информации о решении на базе Windows см. подготовительные процедуры и руководство по эксплуатации Kaspersky Security Center Windows (643.46856491.00069-10 90 02).

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

Таблица 1. Сравнение возможностей программы Kaspersky Security Center на базе Windows и на базе Linux

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 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

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Windows или Linux
Иерархия Серверов администрирования	✓	✓
Иерархия групп администрирования	✓	✓
Опрос сети	✓	✓ (по IP-диапазонам и контроллерам доменов, Samba 4 Active Directory, Microsoft Active Directory)
Максимальное количество управляемых устройств	100000	20 000
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. 351)	✓	✓
Управление безопасностью, ориентированное на пользователя (см. стр. 351)	✓	✓
Политики программ	✓	✓
Задачи для программ "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓
Kaspersky Private Security Network	✓	✓

kaspersky

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
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)
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Вход в консоль с использованием доменной аутентификации	✓	✓ (единый вход (SSO) временно не поддерживается)
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	✓	—

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15 Linux
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	✓	—
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

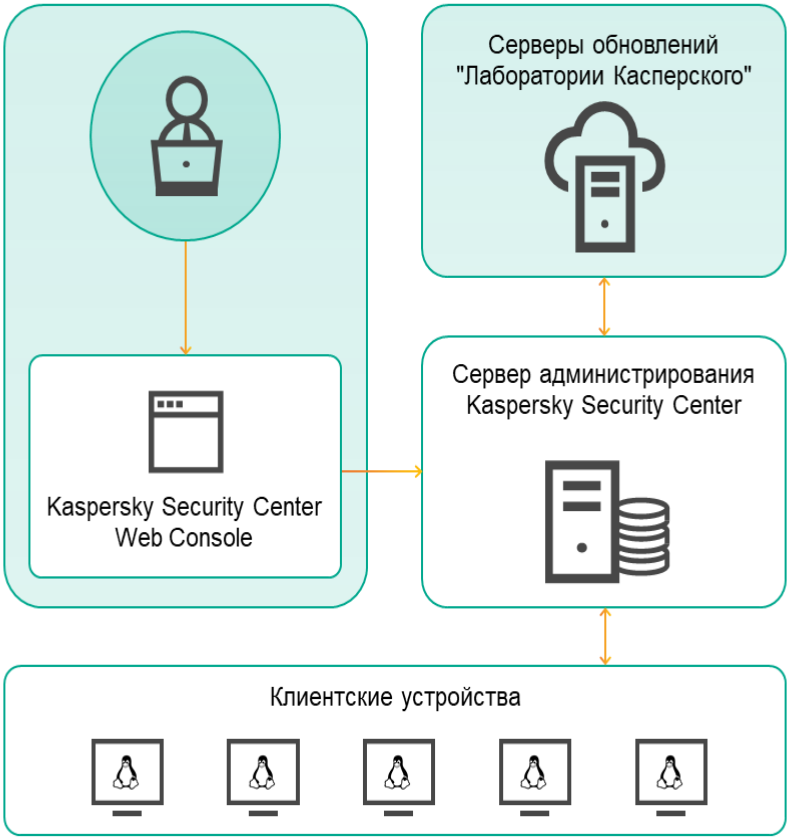
Архитектура и основные понятия

В этом разделе описана архитектура программы и развернутые определения основных понятий, относящихся к программе Kaspersky Security Center.

В этом разделе

Архитектура программы

Этот раздел содержит описание компонентов Kaspersky Security Center и их взаимодействия.



Программа Kaspersky Security Center включает в себя следующие основные компоненты:

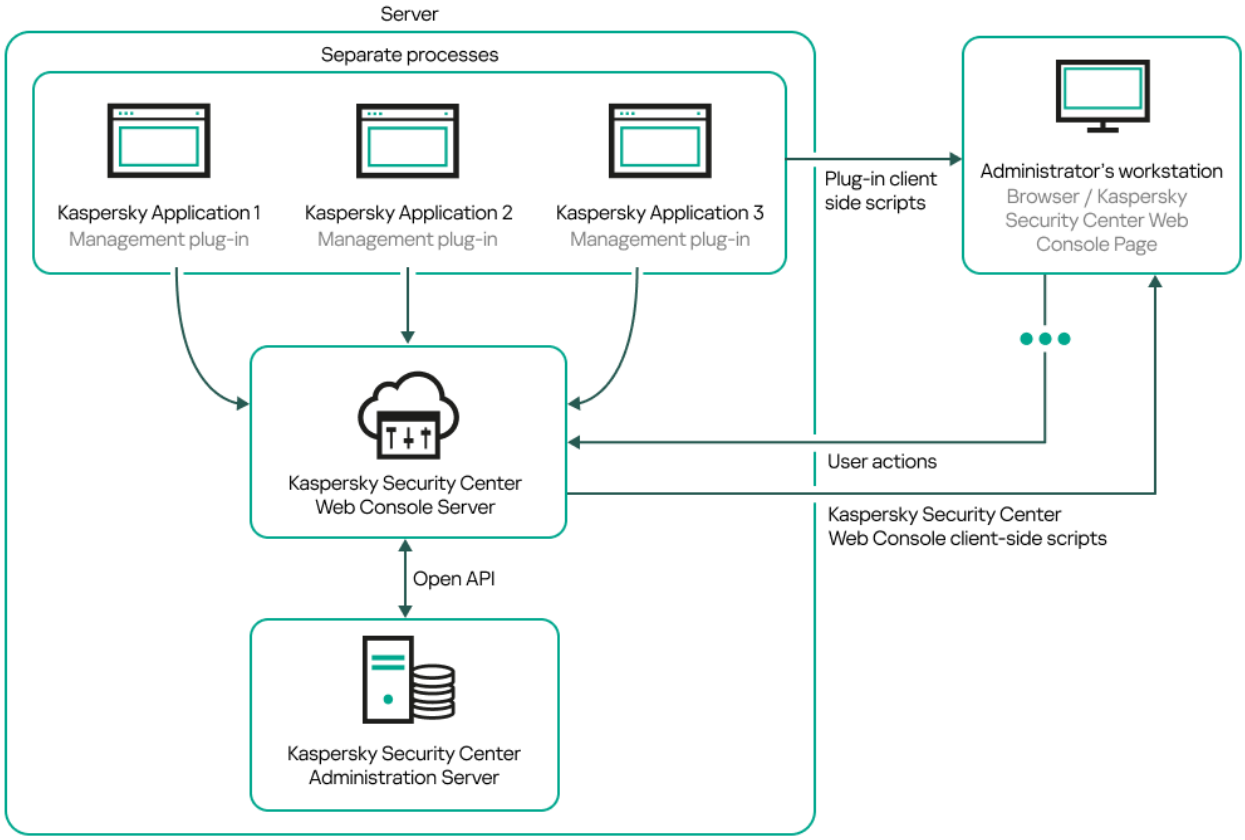
- **Kaspersky Security Center Web Console**. Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.
- **Сервер администрирования Kaspersky Security Center** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.
- **Серверы обновлений "Лаборатории Касперского"**. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.
- **Серверы KSN**. Серверы содержат оперативную базу знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network (см. стр. 399) обеспечивает более высокую скорость реакции программ "Лаборатории

Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

- **Клиентские устройства.** Клиентские устройства организации защищены Kaspersky Security Center. На каждом защищаемом устройстве должно быть установлена одна из программ безопасности "Лаборатории Каперского".

Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center Web Console

На следующем рисунке приведена схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 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 Web Console.

Как администратор, вы имеете доступ к Kaspersky Security Center Web Console через браузер на вашей рабочей станции.

Когда вы выполняете определенные действия в Kaspersky Security Center Web Console, Сервер Kaspersky Security Center Web Console взаимодействует с Сервером администрирования Kaspersky Security Center по OpenAPI. Сервер Kaspersky Security Center Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center и отображает результаты ваших действий в Kaspersky Security Center Web Console.

Порты, используемые Kaspersky Security Center

В таблицах ниже перечислены порты, которые должны быть открыты на Сервере администрирования и на

клиентских устройствах. При необходимости вы можете изменить каждый из этих портов по умолчанию.

Таблица 2. Порты, используемые Сервером администрирования Kaspersky Security Center

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8060	klcsweb	TCP	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить значения портов, заданных по умолчанию, в разделе **Веб-сервер** окна свойств Сервера администрирования.
8061	klcsweb	TCP (TLS)	Передача на клиентские устройства опубликованных инсталляционных пакетов	Публикация инсталляционных пакетов. Вы можете изменить значения портов, заданных по умолчанию, в разделе **Веб-сервер** окна свойств Сервера администрирования.
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. Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения во время установки Kaspersky Security Center (см. стр. 85). Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования (см. стр. 155).
13000	klserver	UDP	Прием информации от Агентов администрирования о выключении устройств	Управление клиентскими устройствами. Вы можете изменить значения портов по умолчанию в окне свойств политики Агента администрирования (см. стр. 382).
13299	klserver	TCP (TLS)	Получение соединений от Kaspersky Security Center Web Console к Серверу администрирования; получение соединений от Сервера администрирования через OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Порты подключения** раздела **Общий**) или при создании иерархии Серверов администрирования (см. стр. 155).

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
14000	klserver	TCP	Прием подключений от Агентов администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию при настройке портов подключения (см. стр. 85) при установке Kaspersky Security Center или при подключении клиентского устройства к Серверу администрирования вручную (см. стр. 123).
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. стр. 400).
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в окне свойств Сервера администрирования (см. стр. 400).
17000	klactprx	TCP (TLS)	Прием подключений для активации программ от управляемых устройств	Прокси-сервер активации для управляемых устройств. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Дополнительные порты** раздела **Общий**).
19170	klserver	HTTPS (TLS)	Туннелирование соединения с управляемыми устройствами с помощью утилиты klsctunnel (см. стр. 152)	Удаленное подключение к управляемым устройствам с помощью Kaspersky Security Center Web Console. Вы можете изменить номер порта, указанного по умолчанию, с помощью утилиты klscflag.

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 MariaDB Server). Подробную информацию см. в документации СУБД.

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 3. 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 Web Console	Kaspersky Security Center Web Console. Вы можете изменить номер порта, указанного по умолчанию, во время установки Kaspersky Security Center Web Console (см. стр. 92). Если вы устанавливаете Kaspersky Security Center 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 4. Порты, используемые Агентом администрирования

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
15000	klnagent	UDP	Сигналы управления от Сервера администрирования или точки распределения к Агентам администрирования	Управление клиентскими устройствами. Вы можете изменить значения портов по умолчанию в окне свойств политики Агента администрирования (см. стр. 382).
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. Вы можете изменить значения портов по умолчанию в окне свойств точки распространения (см. стр. 258).
13001	klnagent	TCP (SSL)	Получение многоадресных запросов от точки распространения, на которой установлен Сервер администрирования	Получение обновлений и инсталляционных пакетов от точки распространения, на которой установлен Сервер администрирования. Вы можете изменить номер порта по умолчанию в окне свойств точки распространения в Консоли администрирования или в Kaspersky Security Center Web Console (см. стр. 258).

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.

Обратите внимание, что рекомендации по совместимости Kaspersky Security Center со сторонним программным обеспечением носят справочный характер и могут быть неприменимы к новым версиям стороннего программного обеспечения. Описанные рекомендации по настройке портов основаны на опыте Службы технической поддержки и наших лучших практиках.

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 5. 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 и шлюзов соединения (см. стр. 258)	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов. Вы можете изменить значения портов по умолчанию в свойствах точки распространения (см. стр. 258).
13111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	TCP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в свойствах точки распространения (см. стр. 258).
15111 (только если на устройстве запущена служба прокси-сервера KSN)	ksnproxy	UDP	Прием запросов от управляемых устройств к прокси-серверу KSN	Прокси-сервер KSN. Вы можете изменить значения портов по умолчанию в свойствах точки распространения (см. стр. 258).

См. также:

Порты, используемые программой Kaspersky Security Center Web Console

В таблице ниже перечислены порты, которые должны быть открыты на устройстве, на котором установлен

Сервер Kaspersky Security Center Web Console (далее также просто Kaspersky Security Center Web Console).

Таблица 6. Порты, используемые программой Kaspersky Security Center 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 плагинов управления.
1329, 2003	KSCWebConsoleManagementService	HTTPS	API-порты, которые используются для получения запросов от службы KSCWebConsole, работающей на том же устройстве.	Обновление компонентов Kaspersky Security Center Web Console.
2005	KSCWebConsole	HTTPS	API-порт, который используется для получения запросов от службы KSCWebConsoleManagementService, работающей на том же устройстве.	Запуск процессов node программы Kaspersky Security Center Web Console.
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 Web Console и обновление компонентов Kaspersky Security Center Web Console.
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	API-порты Message Broker, которые используются для связи между Kaspersky Security Center Web Console и плагинами управления.	Взаимодействие между Kaspersky Security Center Web Console и плагинов управления

См. также:

Порты, используемые Kaspersky Security Center.....45

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 Kaspersky Security Center 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 Web Console, установленную на устройство под управлением Linux, то программа отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов (см. стр. 94).

Вы можете подключиться к Серверу администрирования с помощью Kaspersky Security Center Web Console.

См. также:

Начало работы 78

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.

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования* (см. стр. 53).

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.
- Использование Kaspersky Security Center поставщиками услуг. Поставщику услуг достаточно установить Kaspersky Security Center и Kaspersky Security Center Web Console. Для управления большим числом клиентских устройств различных организаций поставщик услуг может включать в иерархию Серверов администрирования подчиненные Серверы администрирования (включая виртуальные Серверы).

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:

Начало работы 78

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.

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, 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.

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*. Вы можете установить Агент администрирования следующими способами:

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

Во время установки Сервера администрирования, серверная версия Агента администрирования устанавливается автоматически совместно с Сервером администрирования. Для управления устройством с Сервером администрирования рекомендуется установить Агент администрирования для Linux на это устройство https://support.kaspersky.com/help/KES4Linux/11.4.0/ru-RU/237152.htm. В этом случае Агент администрирования для Linux устанавливается и работает независимо от серверной версии Агента администрирования, которая была установлена вместе с Сервером администрирования.

Названия процессов, которые запускает Агент администрирования:

- klnagent64.service (для 64-разрядной операционной системы);
- klnagent.service (для 32-разрядной операционной системы).

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

См. также:

Развертывание Агента администрирования и программы безопасности 209

kaspersky

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.

Управляемое устройство

Управляемое устройство – это устройство с операционной системой Linux, на котором установлен Агент администрирования. 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 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 20 000 устройств.

См. также:

Параметры управляемого устройства 239

Сценарий: Настройка защиты сети 349

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.

kaspersky

Рабочее место администратора

Устройства, на которых установлен Сервер Kaspersky Security Center Web Console, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

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.

Веб-плагин управления

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

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

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач (на стр. 406) и параметров программы.
- Интерфейс для создания и изменения политик и профилей политик (см. стр. 356) для удаленной централизованной настройки программ "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных программами.
- Функции Kaspersky Security Center Web Console для отображения оперативных данных и событий программы, а также статистики, полученной от клиентских устройств.

См. также:

Список поддерживаемых программ "Лаборатории Касперского".....37

Развертывание программ "Лаборатории Касперского".....299

kaspersky

Политики

Политика – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 56) и ее подгруппам. Вы можете установить несколько программ "Лаборатории Касперского" (см. стр. 37) 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:

Таблица 7. 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.
- 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.

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 356
Создание профиля политики 377

Задачи

Kaspersky Security Center управляет работой программ безопасности "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.
- 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 Kaspersky Security Center Web Console, 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 системном журнале событий и журнале событий Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве (см. стр. 535).

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

См. также:

Начало работы 78

Область действия задачи

Область задачи (см. стр. 406) – 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) 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 356

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.

  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.

  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.

- Осуществлять удаленную установку программ "Лаборатории Касперского" и других поставщиков программного обеспечения, в том числе 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, чтобы устройство исполняло роль прокси-сервера KSN (см. стр. 258). В этом случае на устройстве запустится служба прокси-сервера KSN (см. стр. 404).

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 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.

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. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях программы, изменены не будут.

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.

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 проблему

безопасности с уровнем важности *Предупреждение*. Проблема безопасности будет опубликована в свойствах устройства в разделе **Проблемы безопасности**.

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.

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, 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 253

kaspersky

Схемы трафика данных и использования портов

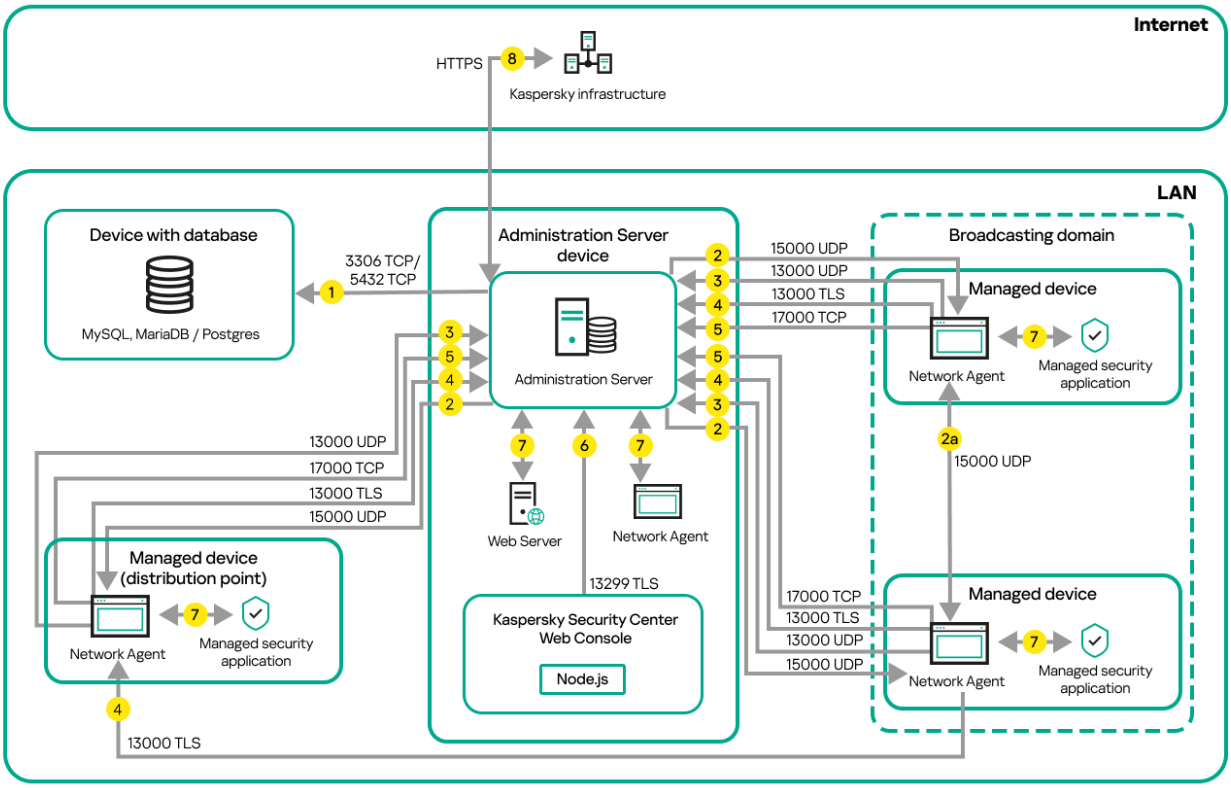
В этом разделе приведены схемы трафика данных между компонентами Kaspersky Security Center, управляемыми программами безопасности и внешними серверами для различных конфигураций. Схемы содержат номера портов, которые должны быть доступны на локальных устройствах.

В этом разделе

См. также:

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. 204). 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. 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 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   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).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь от Сервера администрирования к этим устройствам напрямую не отправляются.

2a. Агенты администрирования на немобильных управляемых устройствах обмениваются данными о других Агентах администрирования в том же широковещательном домене (затем данные отправляются на Сервер администрирования).

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 и от подчиненных Серверов администрирования 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. 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.
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.

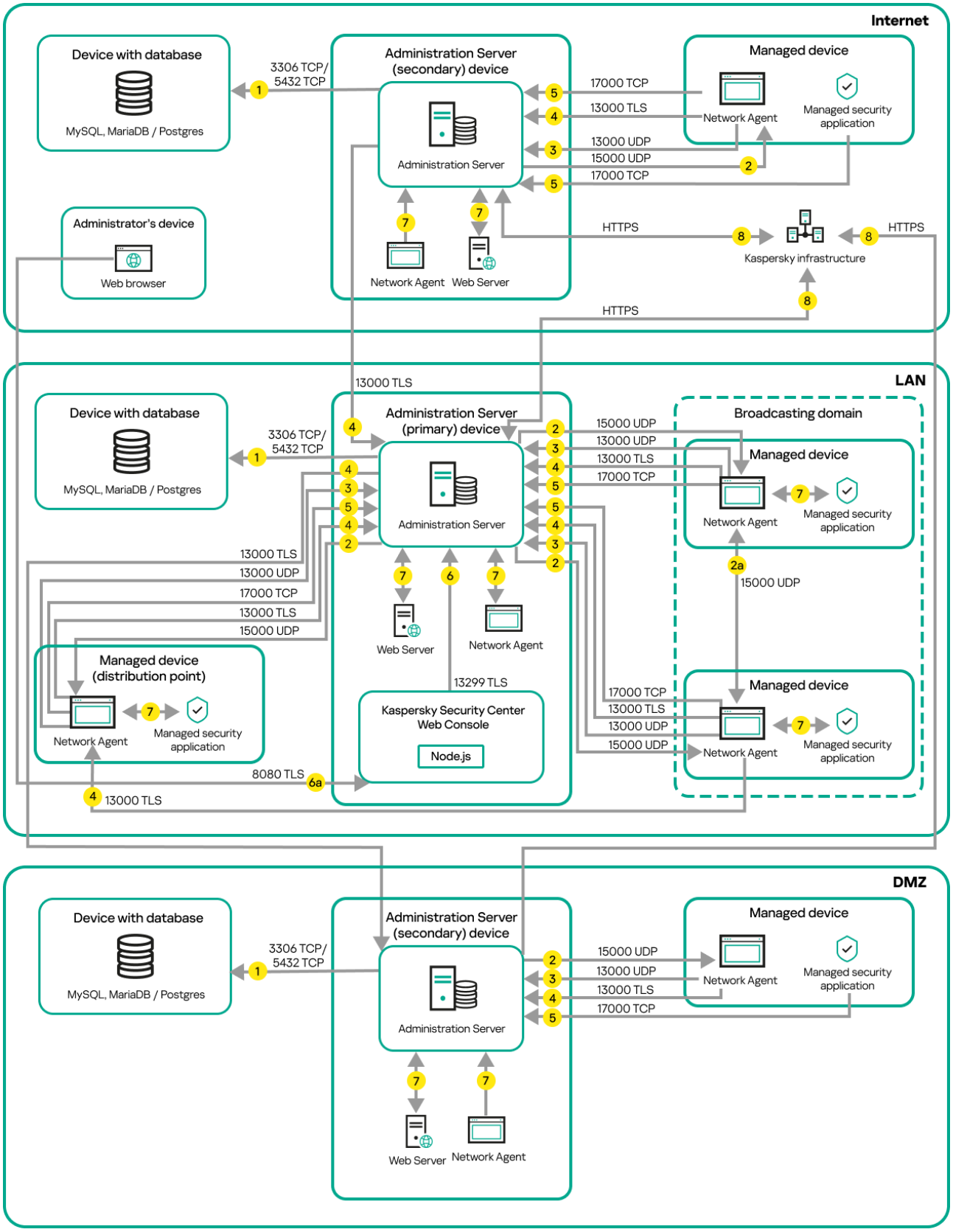
См. также:

Типовая конфигурация: один офис 198

Порты, используемые Kaspersky Security Center 45

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. 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 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   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).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь от Сервера администрирования к этим устройствам напрямую не отправляются.
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 и от подчиненных Серверов администрирования 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. 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.

   6a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
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.

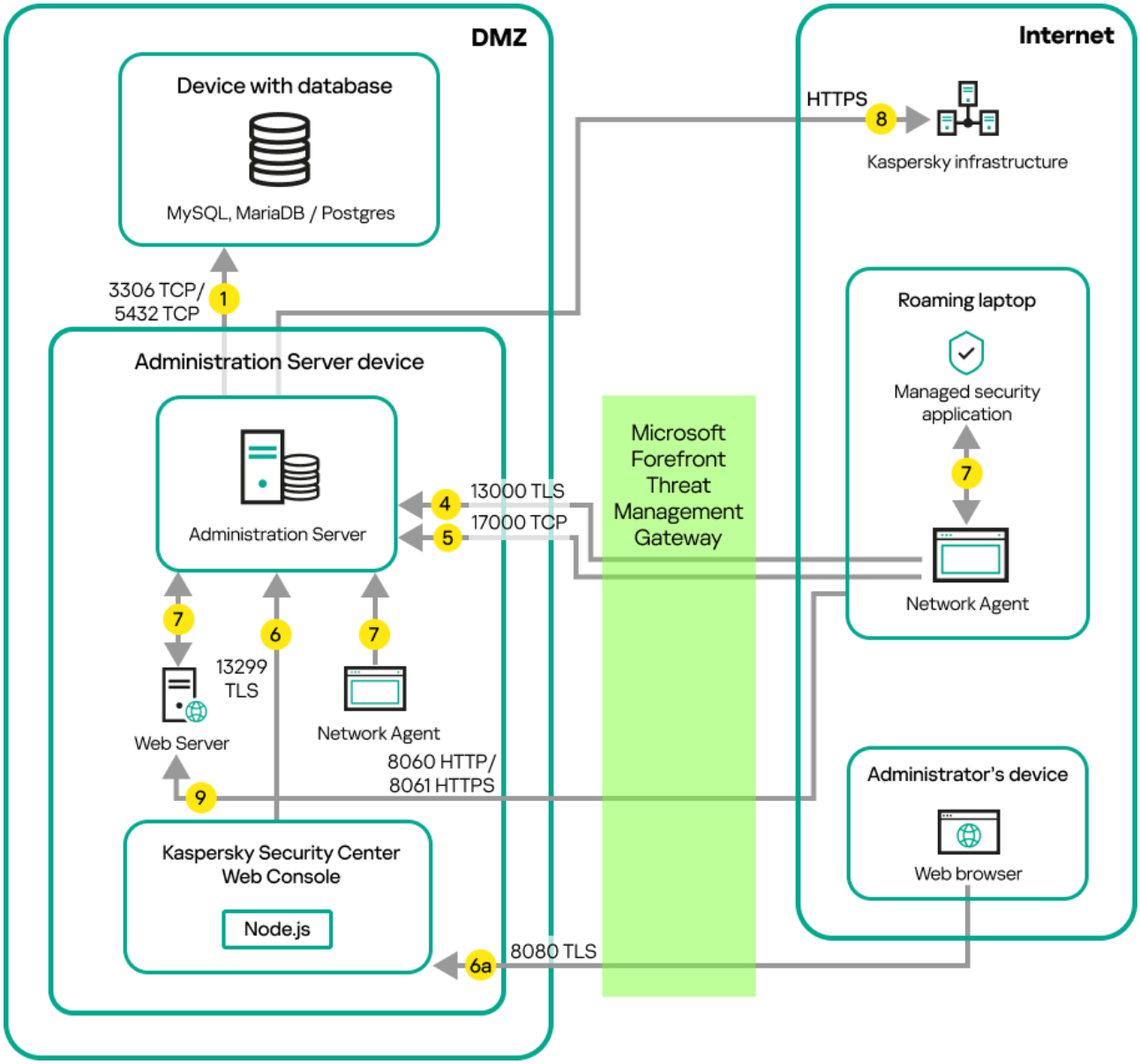
   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вы должны управлять этими данными вручную.

См. также:

Иерархия Серверов администрирования 155
Порты, используемые Kaspersky Security Center 45

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 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. 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 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

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).

Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь от Сервера администрирования к этим устройствам напрямую не отправляются.

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 и от подчиненных Серверов администрирования 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. 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.

   6a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
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. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 54), который находится на том же устройстве, на котором установлен Сервер администрирования.

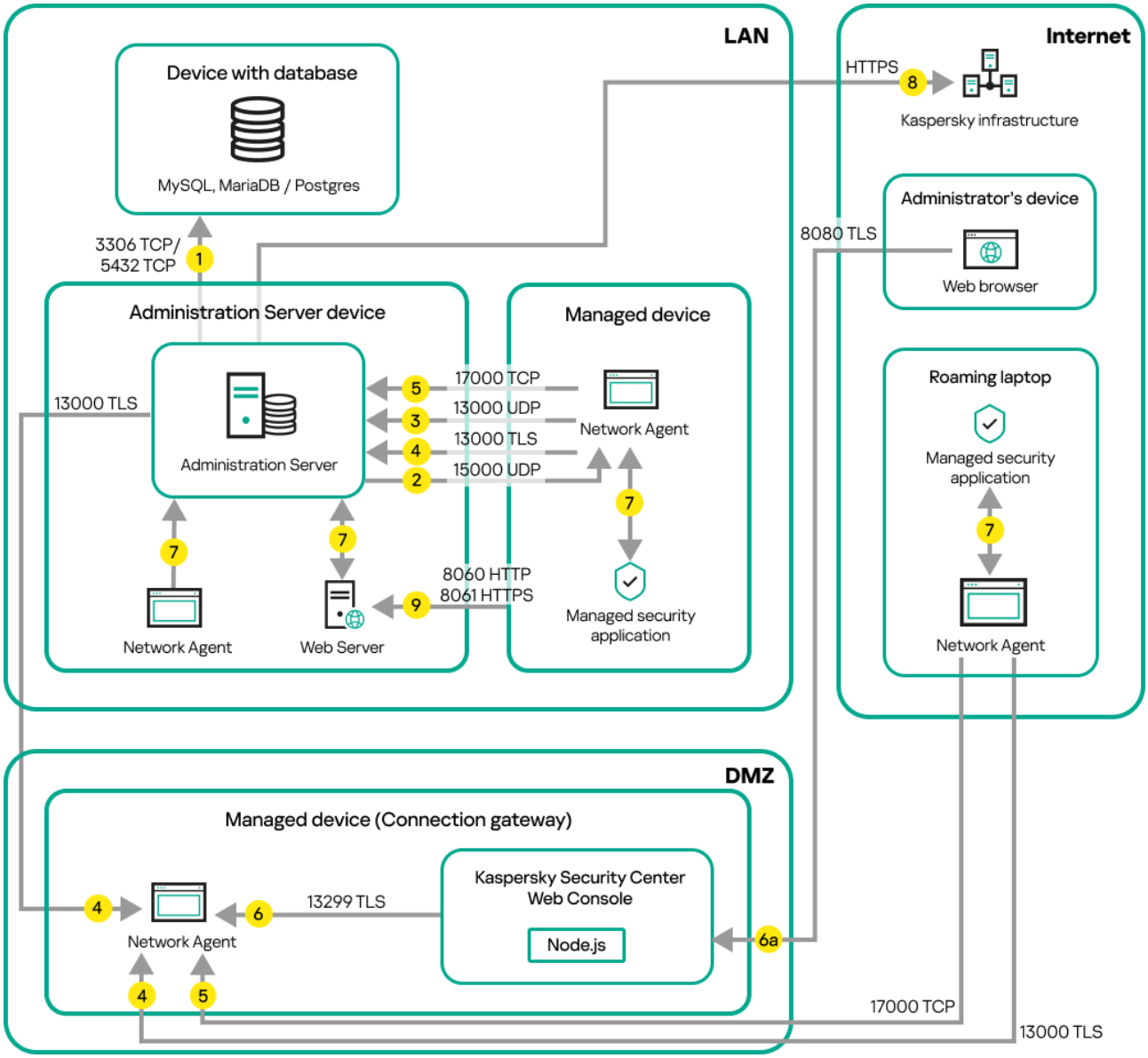
См. также:

Порты, используемые Kaspersky Security Center.....45

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 находятся в интернете. Шлюз соединения используется.

Эта схема развертывания рекомендуется, если вы не хотите, чтобы управляемые 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. 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 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   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).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь от Сервера администрирования к этим устройствам напрямую не отправляются.
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 и от подчиненных Серверов администрирования 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. 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.

   6a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
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.

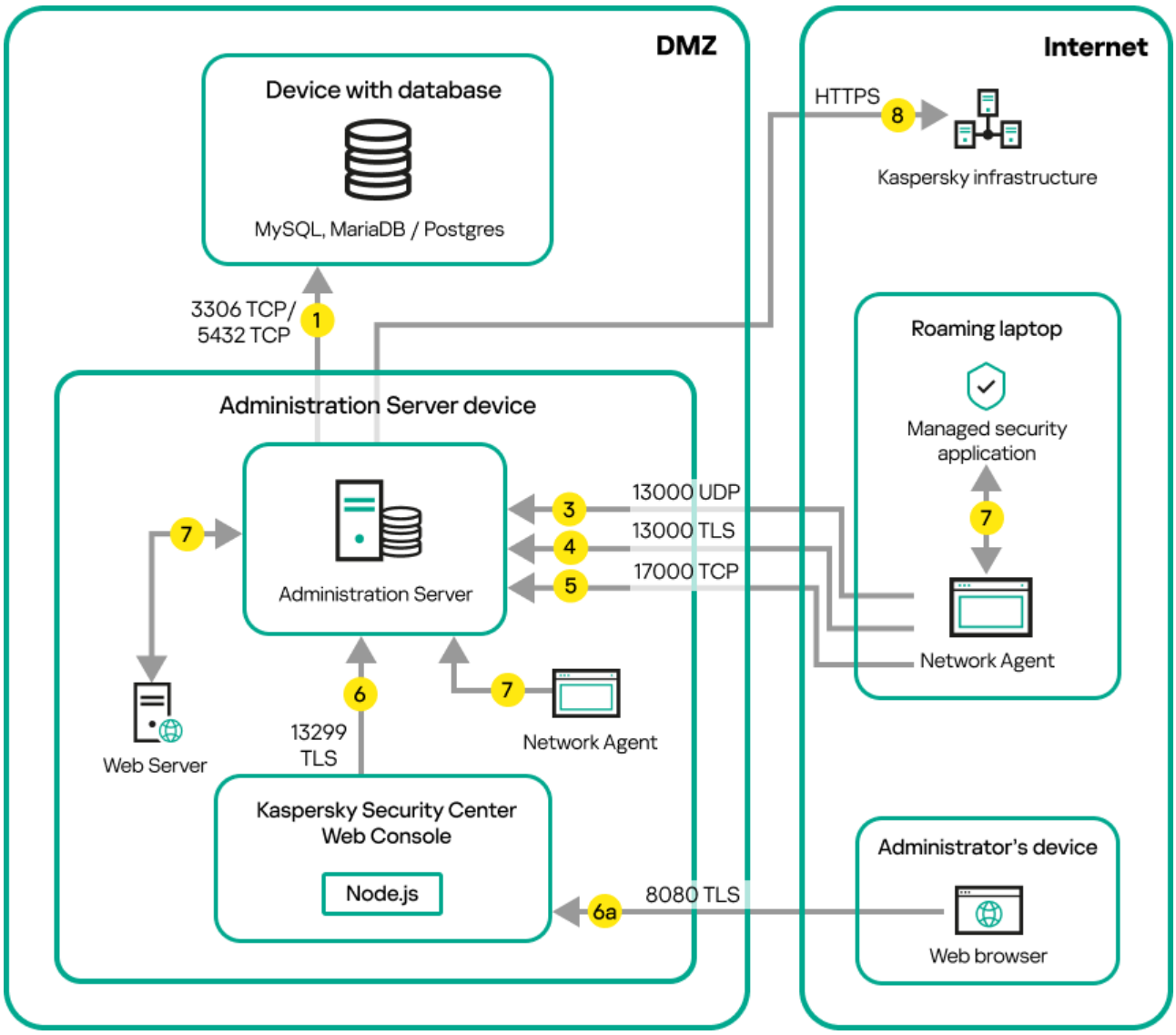
9. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 54), который находится на том же устройстве, на котором установлен Сервер администрирования.

См. также:

Порты, используемые Kaspersky Security Center.....45

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.



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. 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 5432 для PostgreSQL Server или Postgres Pro Server). Подробную информацию см. в документации СУБД.
2. Запросы на связь с Сервером администрирования передаются на все немобильные управляемые устройства через UDP-порт 15000.

   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).

   Если Сервер администрирования не имеет прямого доступа к управляемым устройствам, запросы на связь от Сервера администрирования к этим устройствам напрямую не отправляются.
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 и от подчиненных Серверов администрирования 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 в демилитаризованной зоне также принимает подключение от Сервера администрирования по SSL-порту 13000 (см. стр. 64). 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.
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. 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.

6a. Данные от браузера, установленного на отдельном устройстве администратора, передаются на Сервер Kaspersky Security Center Web Console через TLS-порт 8080. Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

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. Запросы на пакеты от управляемых устройств передаются на Веб-сервер, который находится на том же устройстве, на котором установлен Сервер администрирования (см. стр. 54).

См. также:

Порты, используемые Kaspersky Security Center.....45

Доступ из интернета: Сервер администрирования в демилитаризованной зоне.....201

kaspersky

Начало работы

Следуя этому сценарию, вы установите Сервер администрирования Kaspersky Security Center и Kaspersky Security Center Web Console, выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки, а также установите программы "Лаборатории Касперского" на управляемые устройства с помощью мастера развертывания защиты.

Предварительные требования

У вас должен быть лицензионный ключ (код активации) для Kaspersky Endpoint Security для бизнеса или лицензионные ключи (коды активации) для программ безопасности "Лаборатории Касперского".

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

Этапы

Основной сценарий установки состоит из следующих этапов:

1. Выбор структуры защиты организации

   Ознакомьтесь с компонентами Kaspersky Security Center (см. стр. 43). Исходя из конфигурации сети и пропускной способности каналов связи определите, какое количество Серверов администрирования необходимо использовать и как их разместить по офисам, если вы работаете с распределенной сетью (см. стр. 194).

   Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования (см. стр. 52). 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.

2. 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. 114) и убедитесь, что они соответствуют всем требованиям (см. стр. 116).

3. Установка системы управления базами данных (СУБД)

   Установите СУБД (см. стр. 81), используемую Kaspersky Security Center, или используйте существующую СУБД.

   > 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.

4. Настройка портов

   Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты открыты необходимые порты (см. стр. 45).

   Если требуется предоставить доступ к Серверу администрирования из интернета (см. стр. 200), настройте порты и параметры подключения в зависимости от конфигурации сети.

5. Установка Kaspersky Security Center

Выберите устройство с операционной системой Linux, которое вы собираетесь использовать в качестве Сервера администрирования; убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям (см. стр. 18), и установите на устройство Kaspersky Security Center (см. стр. 85). Вместе с компонентом Сервер администрирования автоматически будет установлена серверная версия Агента администрирования.

6. Установка Kaspersky Security Center Web Console и веб-плагинов управления

   Выберите устройство с операционной системой Linux, которое вы собираетесь использовать в качестве рабочей станции администратора; убедитесь, что аппаратное и программное обеспечение устройства соответствует требованиям (см. стр. 18), и установите на это устройство Kaspersky Security Center Web Console. Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования.

   Загрузите веб-плагин управления Kaspersky Endpoint Security для Linux https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint и установите его на то же устройство, на котором установлена программа Kaspersky Security Center Web Console.

7. Установка Kaspersky Endpoint Security для Linux и Агента администрирования на устройство с Сервером администрирования

   По умолчанию программа не использует устройство с Сервером администрирования как управляемое устройство. Для защиты Сервера администрирования от вирусов и других угроз, а также для управления этим устройством рекомендуется установить Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/233694.htm и Агент администрирования для Linux https://support.kaspersky.com/help/KES4Linux/11.4.0/ru-RU/237152.htm на устройство с Сервером администрирования. В этом случае Агент администрирования для Linux устанавливается и работает независимо от серверной версии Агента администрирования, которая была установлена вместе с Сервером администрирования.

8. Выполнение первоначальной настройки

   После завершения установки Сервера администрирования при первом подключении к Серверу администрирования автоматически запускается Мастер первоначальной настройки (см. стр. 129). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (см. стр. 356) и задачи (см. стр. 406) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. стр. 349).

9. Обнаружение сетевых устройств

   Опросите сеть для обнаружения устройств 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.

10. Объединение устройств в группы администрирования

    В некоторых случаях для развертывания защиты на устройствах сети оптимальным образом может потребоваться разделить устройства на группы администрирования (см. стр. 250) с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам (см. стр. 244) 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.

11. Назначение точек распространения

    Точки распространения для групп администрирования назначаются автоматически, но при необходимости вы можете назначить их вручную (см. стр. 202). Точки распространения рекомендуется использовать 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.

12. Установка Агента администрирования и программ безопасности на устройства в сети

    Развертывание защиты в сети организации подразумевает установку Агента администрирования и программ безопасности (см. стр. 299) 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).

13. Распространение лицензионных ключей на клиентские устройства

    Распространите лицензионные ключи (см. стр. 339) на клиентские устройства, чтобы активировать управляемые программы безопасности на этих устройствах.

14. 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. Управление безопасностью устройств реализуется с помощью политик (см. стр. 356) и задач (см. стр. 406). Задачи могут выполняться только на устройствах, которые соответствуют определенным условиям. Для создания условий отбора устройств используются выборки устройств (см. стр. 272) и теги (см. стр. 285).

15. Мониторинг состояния защиты сети

    Вы можете организовывать мониторинг сети с помощью веб-виджетов на информационной панели (см. стр. 499), формировать отчеты (см. стр. 505) о программах "Лаборатории Касперского", настраивать и просматривать выборки событий (см. стр. 535), полученные от программ на управляемых устройствах, и просматривать список уведомлений.

В этом разделе

kaspersky

Установка

В этом разделе описана установка Kaspersky Security Center и Kaspersky Security Center Web Console.

В этом разделе

Установка системы управления базами данных

Установите систему управления базами данных (СУБД), которая будет использоваться Kaspersky Security Center. Вы можете выбрать одну из поддерживаемых (см. стр. 18) версий 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. 82), PostgreSQL (см. стр. 83) или Postgres Pro (см. стр. 83) используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

kaspersky

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center

Если вы используете сервер MariaDB для Kaspersky Security Center, включите поддержку InnoDB и хранилища MEMORY, а также поддержку кодировок UTF-8 и UCS-2.

Рекомендуемые параметры для файла my.cnf

► *Чтобы настроить файл my.cnf:*

1. Откройте файл my.cnf https://mariadb.com/kb/en/configuring-mariadb-with-option-files/ с помощью текстового редактора.
2. Введите следующие строки в раздел [mysqld] файла my.cnf:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<value>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

Значение `innodb_buffer_pool_size` должно быть не менее 80 процентов от ожидаемого размера базы данных KAV. Обратите внимание, что указанная память выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Если вы используете MariaDB 10.4.3 или более раннюю версию, фактический размер выделенной памяти примерно на 10 процентов превышает указанный размер буфера.

Рекомендуется использовать значение параметра `innodb_flush_log_at_trx_commit=0`, поскольку значения "1" или "2" отрицательно влияют на скорость работы MariaDB.

По умолчанию надстройки оптимизатора `join_cache_incremental`, `join_cache_hashed`, `join_cache_bka` включены. Если эти надстройки не включены, их необходимо включить.

► *Чтобы проверить, включены ли надстройки оптимизатора:*

1. В клиентской консоли MariaDB выполните команду:

```
SELECT @@optimizer_switch;
```

2. Убедитесь, что вывод содержит следующие строки:

```
join_cache_incremental=on
join_cache_hashed=on
```

```
join_cache_bka=on
```

Если эти строки присутствуют и содержат значения `on`, значит, надстройки оптимизатора включены.

Если эти строки отсутствуют или имеют значения `off`, вам необходимо выполнить следующее:

a. Откройте файл my.cnf с помощью текстового редактора.

b. Добавьте в файл my.cnf следующие строки:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

Надстройки `join_cache_incremental`, `join_cache_hash` и `join_cache_bka` включены.

Настройка сервера PostgreSQL или Postgres Pro для работы с Kaspersky Security Center

Kaspersky Security Center поддерживает СУБД PostgreSQL и Postgres Pro. Если вы используете одну из этих СУБД, рассмотрите возможность настройки параметров сервера СУБД для оптимизации работы СУБД с Kaspersky Security Center.

Путь по умолчанию к конфигурационному файлу: /etc/postgresql/<VERSION>/main/postgresql.conf

Рекомендуемые параметры для PostgreSQL и Postgres Pro:

- `shared_buffers =` 25% от объема оперативной памяти устройства, на котором установлена СУБД

  Если оперативной памяти меньше 1 ГБ, то оставьте значение по умолчанию.
- `max_stack_depth =` максимальный размер стека (выполните команду '`ulimit -s`', чтобы получить это значение КБ) минус 1 МБ
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128 MB`

Перезапустите или перезагрузите сервер после обновления файла postgresql.conf, чтобы изменения вступили в силу. Дополнительную информацию см. в документации PostgreSQL https://www.postgresql.org/docs/current/config-setting.html.

Подробнее о том, как создавать и настраивать учетные записи для PostgreSQL и Postgres Pro, см. в следующем разделе: Настройка учетных записей для работы с PostgreSQL и Postgres Pro (см. стр. 112).

Подробную информацию о параметрах сервера PostgreSQL и Postgres Pro, а также о том, как указать эти параметры, см. в соответствующей документации по СУБД.

См. также

Установка системы управления базами данных.....81

Сценарий: Аутентификация PostgreSQL Server

Рекомендуется использовать TLS-сертификат для аутентификации сервера PostgreSQL. Вы можете использовать сертификат аккредитованного центра сертификации (CA) или самоподписанный сертификат. Рекомендуется использовать сертификат аккредитованного центра сертификации (CA), так как самоподписанный сертификат обеспечивает лишь ограниченную защиту.

Сервер администрирования поддерживает как одностороннюю, так и двустороннюю SSL-аутентификацию для PostgreSQL.

Выполните следующие шаги, чтобы настроить SSL-аутентификацию для PostgreSQL:

1. Сгенерируйте сертификат для сервера PostgreSQL.

   Выполните следующие команды:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   ```

   ```
   chmod og-rwx psql.key
   ```

2. Сгенерируйте сертификат для Сервера администрирования.

   Выполните следующие команды. Значение CN должно соответствовать имени пользователя, который подключается к PostgreSQL от имени Сервера администрирования. По умолчанию имя пользователя – postgres.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. Настройте аутентификацию клиентского сертификата.

   Измените pg_hba.conf следующим образом:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   Убедитесь, что в pg_hba.conf нет записи, начинающейся с `host`.

4. Укажите сертификат PostgreSQL.

   Односторонняя SSL-аутентификация

   Двусторонняя SSL-аутентификация

5. Перезапустите демон PostgreSQL.

   Выполните следующую команду:

   ```
   systemctl restart postgresql-14.service
   ```

6. Укажите флаг сервера для Сервера администрирования.

   Односторонняя SSL-аутентификация

   Двусторонняя SSL-аутентификация

7. Перезапустите службу Сервера администрирования.

Установка Kaspersky Security Center

В этом разделе описана установка Kaspersky Security Center.

Перед установкой:

- Установка системы управления базами данных (СУБД) (см. стр. 81).
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).

Используйте установочный файл ksc64_[номер_версии]_amd64.deb или ksc64-[номер_версии].x86_64.rpm, который соответствует дистрибутиву Linux, установленному на вашем устройстве. Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

► *Чтобы установить Kaspersky Security Center:*

1. В командной строке выполните команды, представленные в этой инструкции, под учетной записью root.
2. Создайте группу kladmins и непривилегированную учетную запись ksc. Учетная запись должна быть членом группы kladmins. Для этого последовательно выполните следующие команды:

```
# adduser ksc
# groupadd kladmins
# gpasswd -a ksc kladmins
# usermod -g kladmins ksc
```

3. Запустите установку Kaspersky Security Center. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:
   - `# apt install /<path>/ksc64_[номер_версии]_amd64.deb`
   - `# yum install /<path>/ksc64-[номер_версии].x86_64.rpm -y`
4. Запустите настройку Kaspersky Security Center:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Прочитайте Лицензионное соглашения (см. стр. 330) и Политику конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:
   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center, вы должны принять условия Лицензионного соглашения.
   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center, вы должны принять условия Политики конфиденциальности.
6. При отображении запроса введите следующие параметры:
   a. Введите DNS-имя Сервера администрирования или статический IP-адрес. Для локальной установки – `127.0.0.1`.

b. Введите номер SSL-порта Сервера администрирования. По умолчанию номер порта – 13000.

c. Оцените примерное количество устройств, которыми вы планируете управлять:

- Если у вас от 1 до 100 сетевых устройств, введите 1.
- Если у вас от 101 до 1000 сетевых устройств, введите 2.
- Если у вас более 1000 сетевых устройств, введите 3.

d. Введите имя группы безопасности для служб. По умолчанию используется группа `kladmins`.

e. Введите имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись `ksc`.

f. Введите имя учетной записи, чтобы запустить другие службы. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись `ksc`.

g. Выберите СУБД, которую вы установили для работы с Kaspersky Security Center:

- Если вы установили MySQL или MariaDB, введите 1.
- Если вы установили PostgreSQL или Postgres Pro SQL, введите 2.

h. Введите DNS-имя или IP-адрес устройства, на котором установлена база данных. Для локальной установки – `127.0.0.1`.

i. Введите номер порта базы данных. Этот порт используется для связи с Сервером администрирования. По умолчанию используются следующие порты:

- порт `3306` для MySQL или MariaDB;
- порт `5432` для PostgreSQL или Postgres Pro.

j. Введите имя базы данных.

k. Введите имя учетной записи root базы данных, которая используется для доступа к базе данных.

l. Введите пароль учетной записи root базы данных, которая используется для доступа к базе данных.

Подождите, пока службы добавятся и запустятся автоматически:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Создайте учетную запись, которая будет выполнять роль администратора Сервера администрирования. Введите имя пользователя и пароль. Вы можете использовать следующую команду для создания пользователя: `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <пароль>`

Пароль должен соответствовать следующим правилам:

- Пароль пользователя не может содержать менее 8 или более 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Пользователь добавлен, и Kaspersky Security Center установлен.

Проверка служб

Используйте следующие команды, чтобы проверить, запущена ли служба:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Установка Kaspersky Security Center в тихом режиме

Вы можете установить Kaspersky Security Center на Linux-устройства, используя файл ответов для запуска установки в тихом режиме, то есть без участия пользователя. Файл ответов содержит настраиваемый набор параметров установки: переменные и соответствующие им значения.

Перед установкой:

- Установка системы управления базами данных (СУБД) (см. стр. 81).
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).

Чтобы установить Kaspersky Security Center в тихом режиме:

1. Прочитайте Лицензионное соглашение (см. стр. 330). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Создайте группу "kladmins" и непривилегированную учетную запись "ksc", которая должна быть членом группы "kladmins". Для этого последовательно выполните следующие команды под учетной записью с root-правами:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Создайте файл ответов (в формате TXT) и добавьте список переменных в формате `VARIABLE_NAME=variable_value` в файл ответов. Каждая переменная добавляется на отдельную строку. Файл ответов должен включать переменные, перечисленные в таблице ниже.
4. Задайте значение переменной среды `KLAUTOANSWERS` в корневой среде, содержащей полное имя файла ответов, включая путь, например, с помощью следующей команды:

   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```

5. Запустите установку Kaspersky Security Center в тихом режиме и в зависимости от вашего дистрибутива Linux выполните одну из следующих команд:
   - `# apt install /<path>/ksc64_[номер_версии]_amd64.deb`
   - `# yum install /<path>/ksc64-[номер_версии].x86_64.rpm -y`

6. Создайте учетную запись для работы с Kaspersky Security Center Web Console. Для этого выполните следующую команду под учетной записью с правами root:

   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <пароль>`, где пароль должен содержать хотя бы 8 символов.

Таблица 8. Переменные файла ответов, используемые в качестве параметров установки Kaspersky Security Center в тихом режиме

Имя переменной	Обязательная	Описание	Возможные значения
EULA_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Лицензионного соглашения.	1
PP_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Политики конфиденциальности.	1
KLSRV_UNATT_SERVERADDRESS	Да	DNS-имя Сервера администрирования или статический IP-адрес.	DNS-имя устройства или IP-адрес.
KLSRV_UNATT_PORT_SRV	Нет	Номер порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 14000.	Номер порта
KLSRV_UNATT_PORT_SRV_SSL	Нет	Номер SSL-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13000.	Номер порта
KLSRV_UNATT_PORT_KLOAPI	Нет	Номер KLOAPI-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13299.	Номер порта
KLSRV_UNATT_PORT_GUI	Нет	Номер GUI-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13291.	Номер порта
KLSRV_UNATT_NETRANGETYPE	Нет	Примерное количество устройств, которыми вы планируете управлять. Необязательный параметр. По умолчанию указано значение 1.	1 от 1 до 100 сетевых устройств. 2 от 101 до 1000 сетевых устройств. 3 более 1000 сетевых устройств.
KLSRV_UNATT_DBMS_TYPE	Да	Тип системы управления базой данных: MySQL (MariaDB) или Postgres.	mysql или postgres
KLSRV_UNATT_DBMS_INSTANCE	Да	IP-адрес сервера базы данных.	IP-адрес;
KLSRV_UNATT_DBMS_PORT	Да	Порт сервера базы данных. Значение по умолчанию для MySQL (MariaDB) – 3306; для Postgres – 5432.	3306 или 5432
KLSRV_UNATT_DB_NAME	Да	Имя базы данных.	kav
KLSRV_UNATT_DBMS_LOGIN	Да	Имя пользователя, имеющего доступ к базе данных.	

KLSRV_UNATT_DBMS_PASSWORD	Да	Пароль пользователя, который имеет доступ к базе данных.	
KLSRV_UNATT_KLADMINSGROUP	Да	Имя группы безопасности для служб.	kladmins
KLSRV_UNATT_KLSRVUSER	Да	Имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Да	Имя учетной записи для запуска других служб. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc

Если Сервер администрирования будет развернут как Отказоустойчивый кластер "Лаборатории Касперского" (см. стр. 99), файл ответов должен включать следующие дополнительные переменные:

KLFOC_UNATT_NODE	Да	Номер узла (1 или 2).	1 или 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Да	Точка подключения общей папки состояния.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Да	Точка подключения общей папки данных.	
KLFOC_UNATT_CONN_MODE	Да	Режим подключения отказоустойчивого кластера.	VirtualAdapter Или ExternalLoadBalancer

Если переменная C_UNATT_CONN_MODE имеет значение VirtualAdapter, файл ответов должен включать следующие дополнительные переменные:

KLFOC_UNATT_CONN_MODE_VA_NAME	Требуется одна из этих переменных	Имя виртуального сетевого адаптера.	
KLFOC_UNATT_CONN_MODE_VA_IPV4		IP-адрес виртуального сетевого адаптера.	IP-адрес;
KLFOC_UNATT_CONN_MODE_VA_IPV6		IPv6-адрес виртуального сетевого адаптера.	IPv6-адрес.

Установка Kaspersky Security Center на Astra Linux в режиме замкнутой программной среды

В этом разделе описывается, как установить Kaspersky Security Center на устройство с операционной системой Astra Linux Special Edition.

Перед установкой:

- Установка системы управления базами данных (см. стр. 81).
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).

- Загрузите ключ программы kaspersky_astra_pub_key.gpg https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

Используйте установочный файл ksc64_[номер_версии]_amd64.deb. Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

Выполните команды, представленные в этой инструкции, под учетной записью root.

► *Чтобы установить Kaspersky Security Center 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 директорию, созданную на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

6. Создайте группу kladmins и непривилегированную учетную запись ksc. Учетная запись должна быть членом группы kladmins. Для этого последовательно выполните следующие команды:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

7. Запустите установку Kaspersky Security Center:

   ```
   # apt install /<path>/ksc64_[номер_версии]_amd64.deb
   ```

8. Запустите настройку Kaspersky Security Center:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. Прочитайте Лицензионное соглашения (см. стр. 330) и Политику конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center, вы должны принять условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Введите `n`, если вы не принимаете условия Политики

конфиденциальности. Чтобы использовать Kaspersky Security Center, вы должны принять условия Политики конфиденциальности.

10. При отображении запроса введите следующие параметры:
    a. Введите DNS-имя Сервера администрирования или статический IP-адрес.
    b. Введите номер порта Сервера администрирования. По умолчанию номер порта – 14000.
    c. Введите номер SSL-порта Сервера администрирования. По умолчанию номер порта – 13000.
    d. Оцените примерное количество устройств, которыми вы планируете управлять:
        - Если у вас от 1 до 100 сетевых устройств, введите 1.
        - Если у вас от 101 до 1000 сетевых устройств, введите 2.
        - Если у вас более 1000 сетевых устройств, введите 3.
    e. Введите имя группы безопасности для служб. По умолчанию используется группа kladmins.
    f. Введите имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksc.
    g. Введите имя учетной записи, чтобы запустить другие службы. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksc.
    h. Введите IP-адрес устройства, на котором установлена база данных.
    i. Введите номер порта базы данных. Этот порт используется для связи с Сервером администрирования. По умолчанию номер порта – 3306.
    j. Введите имя базы данных.
    k. Введите имя учетной записи root базы данных, которая используется для доступа к базе данных.
    l. Введите пароль учетной записи root базы данных, которая используется для доступа к базе данных.

    Подождите, пока службы добавятся и запустятся автоматически:
        - `klnagent_srv`
        - `kladminserver_srv`
        - `klactprx_srv`
        - `klwebsrv_srv`
    m. Создайте учетную запись, которая будет выполнять роль администратора Сервера администрирования. Введите имя пользователя и пароль.

    Пароль должен соответствовать следующим правилам:
        - Пароль пользователя должен содержать не менее 8 символов, но не более 16.
        - 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Программа Kaspersky Security Center установлена и пользователь добавлен.

Проверка служб

Используйте следующие команды, чтобы проверить, запущена ли служба:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Установка Kaspersky Security Center Web Console

В этом разделе описано, как установить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) на устройства с операционными системами Linux. Сначала необходимо установить систему управления базами данных (см. стр. 81) и Сервер администрирования Kaspersky Security Center (см. стр. 85).

Если вы устанавливаете Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды, следуйте инструкциям для Astra Linux (см. стр. 97).

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 Web Console:*

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.
2. Прочитайте Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center 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. 94), который содержит параметры для подключения Kaspersky Security Center 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 Web Console на устройство с операционной системой Linux ALT необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

Программа Kaspersky Security Center 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 Web Console из файла .deb, выполните следующую команду:

     ```
     $ sudo dpkg -i ksc-web-console-[номер_версии].x86_64.deb
     ```

   - Чтобы установить Kaspersky Security Center Web Console из файла .rpm, выполните одну из следующих команд:

     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[номер_сборки].x86_64.rpm
     ```

     Или

     ```
     $ sudo alien -i 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 Web Console устанавливается в следующую директорию: /var/opt/kaspersky/ksc-web-console.

5. Перезапустите все службы Kaspersky Security Center Web Console, выполнив следующую команду:

   ```
   $ sudo systemctl restart KSC*
   ```

После завершения установки вы можете использовать браузер, чтобы открыть Kaspersky Security Center Web Console и осуществить вход (см. стр. 124).

kaspersky

Параметры установки Kaspersky Security Center Web Console

Для установки Сервера Kaspersky Security Center Web Console на устройства с операционными системами Linux (см. стр. 92) необходимо создать файл ответов (файл .json), который содержит параметры подключения Kaspersky Security Center 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 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 9. Параметры установки Kaspersky Security Center Web Console на устройствах с операционными системами Linux

Параметр	Описание	Доступные значения
address	Адрес Сервера Kaspersky Security Center Web Console (обязательный параметр).	Строковое значение.
port	Номер порта, который Сервер Kaspersky Security Center Web Console использует для подключения к Серверу администрирования (обязательный параметр).	Числовое значение.

Параметр	Описание	Доступные значения
`defaultLangId`	Язык пользовательского интерфейса (по умолчанию `1033`).	Числовой код языка: • Немецкий: `1031` • Английский: `1033` • Испанский: `3082` • Испанский (Мексика): `2058` • Французский: `1036` • Японский: `1041` • Казахский: `1087` • Польский: `1045` • Португальский (Бразилия): `1046` • Русский: `1049` • Турецкий: `1055` • Упрощенный китайский: `4` • Традиционный китайский: `31748` Если значение не указано, используется английский язык (en-US).
`enableLog`	Включение или отключение журнала активности Kaspersky Security Center Web Console.	Логическое значение: • `true` – включение журнала активности (выбрано по умолчанию). • `false` – выключение журнала активности.
`trusted`	Список доверенных Серверов администрирования, которым разрешено подключаться к Kaspersky Security Center Web Console. Для каждого Сервера администрирования должны быть заданы следующие параметры: • адрес Сервера администрирования; • порт OpenAPI, который используется программой Kaspersky Security Center Web Console для подключения к Серверу администрирования (по умолчанию 13299); • путь к сертификату Сервера администрирования; • имя Сервера администрирования, которое будет отображаться в окне входа. 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"`. 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. 330). Файл, содержащий условия Лицензионного соглашения, загружается вместе с установочным файлом.	Логическое значение: • true – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения (см. стр. 330). • false – Я не принимаю условия Лицензионного соглашения (выбрано по умолчанию). Если значение не указано, программа установки Kaspersky Security Center Web Console отобразит Лицензионное соглашение и спросит, согласны ли вы принять условия Лицензионного соглашения.
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. 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 (см. стр. 45).	Строковое значение следующего формата: "group name:user name". Пример: "Group1:User1". Если значение не указано, установщик Kaspersky Security Center Web Console создает по умолчанию учетную запись user_management_%uid%.
managementServiceAccount	Учетная запись, от имени которой работает служба KSCWebConsoleManagement (см. стр. 45).	Строковое значение следующего формата: "group name:user name". Пример: "Group1:User1". Если значение не указано, установщик Kaspersky Security Center Web Console создает по умолчанию учетную запись user_nodejs_%uid%.
serviceWebConsoleAccount	Учетная запись, от имени которой работает служба KSCSvcWebConsole (см. стр. 45).	Строковое значение следующего формата: "group name:user name". Пример: "Group1:User1". Если значение не указано, установщик Kaspersky Security Center Web Console создает по умолчанию учетную запись user_svc_nodejs_%uid%.
pluginAccount	Учетная запись, от имени которой работает служба KSCWebConsolePlugin (см. стр. 45).	Строковое значение следующего формата: "group name:user name". Пример: "Group1:User1". Если значение не указано, установщик Kaspersky Security Center Web Console создает по умолчанию учетную запись user_web_plugin_%uid%.

Параметр	Описание	Доступные значения
messageQueueAccount	Учетная запись, от имени которой работает служба KSCWebConsoleMessageQueue (см. стр. 45).	Строковое значение следующего формата: "group name:user name". Пример: "Group1:User1". Если значение не указано, установщик Kaspersky Security Center 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 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.....45

Установка Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды

В этом разделе описано, как установить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) на устройства с операционной системой Astra Linux Special Edition. Сначала необходимо установить систему управления базами данных (см. стр. 81) и Сервер администрирования Kaspersky Security Center (см. стр. 85).

► *Чтобы установить Kaspersky Security Center Web Console:*

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.
2. Прочитайте Лицензионное соглашение. Если в состав дистрибутива Kaspersky Security Center 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. 94), который содержит параметры для подключения Kaspersky Security Center 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.cer|KSC Server",
  "acceptEula": true
}
```

4. Откройте файл /etc/digsig/digsig_initramfs.conf и укажите следующие параметры:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. В командной строке введите следующую команду, чтобы установить совместимый пакет:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Создайте директорию для ключа программы:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Поместите ключ программы в директорию /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg, созданную на предыдущем шаге:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Если в комплект поставки Kaspersky Security Center не входит ключ kaspersky_astra_pub_key.gpg, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

9. Под учетной записью с правами root используйте командную строку для запуска установочного файла. Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

   - Чтобы установить или обновить предыдущую версию Kaspersky Security Center Web Console, выполните следующую команду:

     ```
     $ sudo dpkg -i ksc-web-console-[номер_версии].x86_64.deb
     ```

   - Чтобы обновить предыдущую версию Kaspersky Security Center Web Console, выполните следующую команду:

     ```
     $ sudo dpkg -i ksc-web-console-[номер_сборки].x86_64.deb
     ```

   Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки. Kaspersky Security Center Web Console устанавливается в следующую директорию: /var/opt/kaspersky/ksc-web-console.

10. Перезапустите все службы Kaspersky Security Center Web Console, выполнив следующую команду:

    ```
    $ sudo systemctl restart KSC*
    ```

После завершения установки вы можете использовать браузер, чтобы открыть Kaspersky Security Center Web Console и осуществить вход (см. стр. 124).

kaspersky

Установка Kaspersky Security Center Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера "Лаборатории Касперского"

В этом разделе описывается установка Сервера Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console), который подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера "Лаборатории Касперского". Перед установкой Kaspersky Security Center Web Console установите систему управления базами данных (см. стр. 81) и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 105).

► *Чтобы установить Kaspersky Security Center Web Console, которая подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера "Лаборатории Касперского":*

1. Выполните шаг 1 и шаг 2 из раздела Установка Kaspersky Security Center Web Console (см. стр. 92).
2. На шаге 3 в файле ответов (см. стр. 94), укажите `доверенный` параметр установки, разрешающий отказоустойчивому кластеру "Лаборатории Касперского" подключаться к Kaspersky Security Center Web Console. Строковое значение этого параметра имеет следующий формат:

   ```
   "trusted": "server address|port|certificate path|server name"
   ```

   Укажите компоненты `доверенного` параметра установки:

   - **Адрес Сервера администрирования**. Если вы создали дополнительный сетевой адаптер при подготовке узлов кластера, используйте IP-адрес адаптера в качестве адреса отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 103). В противном случае укажите IP-адрес стороннего балансировщика нагрузки, который вы используете.
   - **Порт Сервера администрирования**. Порт OpenAPI, который Kaspersky Security Center 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. 102). 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 Web Console. Укажите локальный путь к сертификату Сервера администрирования.
   - **Имя Сервера администрирования**. Имя отказоустойчивого кластера "Лаборатории Касперского", которое будет отображаться в окне входа в Kaspersky Security Center Web Console.
3. Продолжите стандартную установку Kaspersky Security Center Web Console.

После завершения установки на рабочем столе появляется ярлык и вы можете войти в Kaspersky Security Center Web Console (см. стр. 124).

Вы можете перейти в раздел **Обнаружение устройств и развертывание → Нераспределенные устройства**, чтобы просмотреть информацию об узлах кластера и о файловом сервере (см. стр. 102).

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.

kaspersky

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 для отказоустойчивого кластера (см. стр. 101).

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

1. Создание учетных записей для служб Kaspersky Security Center

   Выполните следующие шаги на активном узле, пассивном узле и файловом сервере:

   Создайте доменную группу с именем "kladmins" и назначьте один и тот же GID всем трем группам. Предоставьте права локального администратора группам.

   Создайте учетную запись с именем "ksc" и назначьте один и тот же UID всем трем учетным записям пользователей. Добавьте учетные записи в доменную группу "kladmins".

   Создайте учетную запись с именем "rightless" и назначьте один и тот же UID всем трем учетным записям пользователей. Добавьте учетные записи в доменную группу "kladmins".

2. 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. 102).

3. 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. 103).

4. Установка системы управления базами данных (СУБД)

   У вас есть два варианта:

   Если вы хотите использовать MariaDB Galera Cluster, выделенный компьютер для СУБД не требуется. Установите кластер MariaDB Galera на каждый из узлов.

   Если вы хотите использовать любую другую поддерживаемую СУБД, установите выбранную СУБД на выделенный компьютер (см. стр. 18).

5. 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 Web Console на отдельном устройстве, не являющемся узлом кластера (см. стр. 99).

6. 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. 101).

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.

На отказоустойчивом кластере "Лаборатории Касперского" все службы Kaspersky Security Center управляются автоматически. Не пытайтесь перезапускать службы вручную.

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 под управлением Linux с файловой системой EXT4. 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). Если вы используете MariaDB Galera Cluster в качестве СУБД, выделенный компьютер для этой цели не требуется.

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. 108).
- 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.

Подготовка файлового сервера для отказоустойчивого кластера "Лаборатории Касперского"

Файловый сервер работает как обязательный компонент отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 101).

► *Чтобы подготовить файловый сервер:*

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям (см. стр. 101).
2. Установите и настройте NFS-сервер:
   - Доступ к файловому серверу должен быть включен для обоих узлов в параметрах NFS-сервера.
   - NFS-протокол должен иметь версию 4.0 или 4.1.
   - Минимальные требования для ядра Linux:
     - 3.19.0-25, если вы используете NFS 4.0;
     - 4.4.0-176, если вы используете NFS 4.1.
3. На файловом сервере создайте две папки и дайте доступ к ним с помощью NFS. 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. 85).

   Выполните следующие команды:

```
sudo yum install nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
```

```
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_sub-
tree_check,no_root_squash\) >> /etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\(rw,sync,no_sub-
tree_check,no_root_squash\) >> /etc/exports"
sudo cat /etc/exports
sudo exportfs -a
sudo systemctl start rpcbind
sudo service nfs start
```

Включите автозапуск, выполнив следующую команду:

```
sudo systemctl enable rpcbind
```

4. Перезапустите файловый сервер.

Файловый сервер подготовлен. Чтобы развернуть отказоустойчивый кластер "Лаборатории Касперского", следуйте инструкциям этого сценария (см. стр. 100).

См. также:

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. 101).

► *Чтобы подготовить узлы для отказоустойчивого кластера "Лаборатории Касперского":*

1. Убедитесь, что у вас есть два компьютера, соответствующих аппаратным и программным требованиям (см. стр. 101). Эти компьютеры будут действовать как активные и пассивные узлы отказоустойчивого кластера.
2. Чтобы узлы работали как клиенты NFS, установите пакет nfs-utils на каждом узле.

   Выполните следующую команду:

   ```
   sudo yum install nfs-utils
   ```

3. Создайте точки подключения, выполнив следующие команды:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Убедитесь, что общие папки могут быть успешно подключены. (Необязательный шаг)

   Выполните следующие команды:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {сер-
   вер}:{путь к папке KlFocStateShare} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {сер-
   вер}:{путь к папке KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc
   ```

Здесь {сервер}:{путь к папке KlFocStateShare} и {сервер }:{путь к папке KlFocDataShare_klfoc} – сетевые пути к общим папкам на файловом сервере.

После успешного подключения общих папок отключите их, выполнив следующие команды:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. Сопоставьте точки подключения и общие папки:

```
sudo vi /etc/fstab
{сервер}:{путь к папке KlFocStateShare} /mnt/KlFocStateShare nfs vers=4,no-
lock,local_lock=none,auto,user,rw 0 0
{сервер}:{путь к папке KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

Здесь {сервер}:{путь к папке KlFocStateShare} и {сервер }:{путь к папке KlFocDataShare_klfoc} – сетевые пути к общим папкам на файловом сервере.

6. Перезапустите оба узла.
7. Подключите общие папки, выполнив следующие команды:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. Убедитесь, что разрешения на доступ к общим папкам принадлежат ksc:kladmins.

   Выполните следующую команду:

```
sudo ls -la /mnt/
```

9. На каждом из узлов настройте дополнительный сетевой адаптер.

   Дополнительный сетевой адаптер может быть физическим или виртуальным. Если вы хотите использовать физический сетевой адаптер, подключите и настройте его стандартными средствами операционной системы. Если вы хотите использовать виртуальный сетевой адаптер, создайте его с помощью программ сторонних производителей

   Выполните одно из следующих действий:

   - Используйте виртуальный сетевой адаптер.
     a. Введите следующую команду, чтобы убедиться, что NetworkManager используется для управления физическим адаптером:

        ```
        nmcli device status
        ```

        Если в выходных данных физический адаптер отображается как неуправляемый, настройте NetworkManager для управления физическим адаптером. Точные шаги настройки зависят от вашего дистрибутива.

     b. Используйте следующую команду для идентификации интерфейсов:

        ```
        ip a
        ```

     c. Создайте профиль конфигурации:

        ```
        nmcli connection add type macvlan dev <физический интерфейс> mode
        bridge ifname <виртуальный интерфейс> ipv4.addresses <маска ад-
        реса> ipv4.method manual autoconnect no
        ```

   - Используйте физический сетевой адаптер или гипервизор. В этом случае отключите программное обеспечение NetworkManager.

a. Удалите соединения NetworkManager для целевого интерфейса:

```
nmcli con del <имя соединения>
```

Используйте следующую команду, чтобы проверить, есть ли подключения к целевому интерфейсу:

```
nmcli con show
```

b. Измените файл NetworkManager.conf. Найдите раздел файла ключа и назначьте целевой интерфейс параметру unmanaged-devices.

```
[keyfile]
unmanaged-devices=interface-name:<имя интерфейса>
```

c. Перезапустите NetworkManager:

```
systemctl reload NetworkManager
```

Чтобы проверить, что целевой интерфейс больше не является управляемым, используйте следующую команду:

```
nmcli dev status
```

- 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.

Узлы подготовлены. Чтобы развернуть отказоустойчивый кластер "Лаборатории Касперского", следуйте инструкциям сценария (см. стр. 100).

См. также:

Об отказоустойчивом кластере "Лаборатории Касперского".....101

Сценарий: Развертывание отказоустойчивого кластера "Лаборатории Касперского".....100

Установка Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского"

Эта процедура описывает, как установить Kaspersky Security Center на узлы отказоустойчивого кластера "Лаборатории Касперского" (см. стр. 101). 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.

Используйте установочный файл ksc64_[номер_версии]_amd64.deb или ksc64-[номер_версии].x86_64.rpm, который соответствует дистрибутиву Linux, установленному на вашем устройстве. Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

kaspersky

Только пользователь из доменной группы KLAdmins может установить Kaspersky Security Center на каждый узел.

Установка на основной (активный) узел

► *Чтобы установить Kaspersky Security Center на основном узле:*

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).
2. В командной строке выполните команды, представленные в этой инструкции, под учетной записью root.
3. Запустите установку Kaspersky Security Center. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:
   - `sudo apt install /<path>/ksc64_[номер_версии]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[номер_версии].x86_64.rpm -y`
4. Запустите настройку Kaspersky Security Center:

   `sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`
5. Прочитайте Лицензионное соглашения (см. стр. 330) и Политику конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:
   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center, вы должны принять условия Лицензионного соглашения.
   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center, вы должны принять условия Политики конфиденциальности.
6. Выберите значение **Основной узел кластера**, в качестве режима установки Сервера администрирования.
7. При отображении запроса введите следующие параметры:
   a. Введите локальный путь к точке подключения общей папки состояния.
   b. Введите локальный путь к точке подключения общей папки данных.
   c. Выберите режим подключения отказоустойчивого кластера: через дополнительный сетевой адаптер или внешний балансировщик нагрузки.
   d. Если вы используете дополнительный сетевой адаптер, введите его имя.
   e. При появлении запроса на ввод DNS-имени или статического IP-адреса Сервера администрирования введите IP-адрес дополнительного сетевого адаптера или IP-адрес внешнего балансировщика нагрузки.
   f. Введите номер SSL-порта Сервера администрирования. По умолчанию номер порта – 13000.
   g. Оцените примерное количество устройств, которыми вы планируете управлять:

- Если у вас от 1 до 100 сетевых устройств, введите 1.
- Если у вас от 101 до 1000 сетевых устройств, введите 2.
- Если у вас более 1000 сетевых устройств, введите 3.

h. Введите имя группы безопасности для служб. По умолчанию используется группа kladmins.

i. Введите имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksc.

j. Введите имя учетной записи, чтобы запустить другие службы. Учетная запись должна быть членом указанной группы безопасности. По умолчанию используется учетная запись ksc.

k. Выберите СУБД, которую вы установили для работы с Kaspersky Security Center:

- Если вы установили MySQL или MariaDB, введите 1.
- Если вы установили PostgreSQL или Postgres Pro SQL, введите 2.

l. Введите DNS-имя или IP-адрес устройства, на котором установлена база данных.

m. Введите номер порта базы данных. Этот порт используется для связи с Сервером администрирования. По умолчанию используются следующие порты:

- порт 3306 для MySQL или MariaDB;
- порт 5432 для PostgreSQL или Postgres Pro.

n. Введите имя базы данных.

o. Введите имя учетной записи root базы данных, которая используется для доступа к базе данных.

p. Введите пароль учетной записи root базы данных, которая используется для доступа к базе данных.

Подождите, пока службы добавятся и запустятся автоматически:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. Создайте учетную запись, которая будет выполнять роль администратора Сервера администрирования. Введите имя пользователя и пароль. Пароль пользователя не может содержать менее 8 или более 16 символов.

Пользователь добавлен, и Kaspersky Security Center установлен первичном узле.

Установка на вторичном (пассивном) узле

► *Чтобы установить Kaspersky Security Center на вторичный узел:*

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).
2. В командной строке выполните команды, представленные в этой инструкции, под учетной записью root.
3. Запустите установку Kaspersky Security Center. В зависимости от вашего дистрибутива Linux выполните одну из следующих команд:

- `sudo apt install /<path>/ksc64_[номер_версии]_amd64.deb`
- `sudo yum install /<path>/ksc64-[номер_версии].x86_64.rpm -y`

4. Запустите настройку Kaspersky Security Center:

   `sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`

5. Прочитайте Лицензионное соглашения (см. стр. 330) и Политику конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:

   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center, вы должны принять условия Лицензионного соглашения.

   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center, вы должны принять условия Политики конфиденциальности.

6. Выберите **Вторичный узел кластера** как режим установки Сервера администрирования.
7. При появлении запроса введите локальный путь к точке подключения общей папки состояния.

Программа Kaspersky Security Center установлена на вторичном узле.

Проверка служб

Используйте следующие команды, чтобы проверить, запущена ли служба:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Теперь вы можете протестировать отказоустойчивый кластер "Лаборатории Касперского", чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

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 /opt/kaspersky/ksc64/sbin.
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 /opt/kaspersky/ksc64/sbin.
3. Откройте командную строку и отключите узел от кластера, выполнив команду `detach_node.sh`.
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 узле, который обслуживался, перейдите в /opt/kaspersky/ksc64/sbin.
8. Откройте командную строку и подключите узел к кластеру, выполнив команду `attach_node.sh`.
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".....101

Сценарий: Развертывание отказоустойчивого кластера "Лаборатории Касперского".....100

Учетные записи для работы с СУБД

Для установки Сервера администрирования и работы с ним требуется внутренняя учетная запись СУБД. Эта учетная запись позволяет вам получить доступ к СУБД. Для такой учетной записи требуются определенные права. Набор необходимых прав зависит от следующих критериев:

- Тип СУБД:
  - MySQL или MariaDB.
  - PostgreSQL или Postgres Pro
- 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 программы установки Сервера администрирования (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 правах на СУБД, которые требуется предоставить учетным записям перед установкой и запуском Сервера администрирования.

MySQL и MariaDB

Если вы выбираете MySQL или MariaDB в качестве СУБД, создайте внутреннюю учетную запись СУБД для доступа к СУБД, а затем предоставьте этой учетной записи необходимые права. Обратите внимание, что способ создания базы данных не влияет на набор прав. Необходимые права перечислены ниже:

- Схема привилегий:
  - База данных Сервера администрирования: ALL (кроме GRANT OPTION).
  - Схемы системы (mysql и sys): SELECT, SHOW VIEW.
  - 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).
- Глобальные привилегии для всех схем: PROCESS, SUPER.

Подробнее о настройке прав учетной записи см. в разделе Настройка учетной записи СУБД для работы с MySQL и MariaDB (см. стр. 111).

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.

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. в разделе Настройка учетной записи СУБД для работы с PostgreSQL или Postgres Pro (см. стр. 112).

Таблица 10. Права роли Postgres

Автоматическое создание базы данных		Создание базы данных вручную
Пользователю *Postgres* не требуются дополнительные права.	Privileges for a new role: CREATEDB.**=ИК: не критично, но это список из одного пункта**	Для новой роли: • Права доступа к базе данных Сервера администрирования: ALL. • Права доступа ко всем таблицам в общедоступной схеме: ALL. • Права доступа ко всем последовательностям в общедоступной схеме: ALL.

Настройка прав на восстановление данных Сервера администрирования

Чтобы восстановить данные Сервера администрирования из резервной копии, роль Postgres, используемая для доступа к СУБД, должна иметь права владельца на базу данных Сервера администрирования.

kaspersky

Настройка учетной записи СУБД для работы с MySQL и MariaDB

Предварительные требования

Прежде чем назначать права учетной записи СУБД, выполните следующие действия:

1. Убедитесь, что вы входите в систему под учетной записью локального администратора.
2. Установите среду для работы с MySQL или MariaDB.

Настройка учетной записи СУБД для установки Сервера администрирования

► *Чтобы настроить учетную запись СУБД 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.

   Чтобы создать учетную запись СУБД с паролем, выполните следующую команду:

   ```
   /* Создайте пользователя с именем KSCAdmin и укажите пароль для KSCAdmin */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<password>';
   ```

   Если вы используете MySQL 8.0 или более раннюю версию в качестве СУБД, обратите внимание, что для этих версий аутентификация "Кеширование пароля SHA2" не поддерживается. Измените аутентификацию по умолчанию с "Кеширование пароля SHA2" на "Собственный пароль MySQL":

   - Чтобы создать учетную запись СУБД, использующую "Собственный пароль MySQL", выполните следующую команду:

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY
     '<password>';
     ```

   - Чтобы изменить аутентификацию для существующей учетной записи СУБД, выполните следующую команду:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY
     '<password>';
     ```

3. Предоставьте следующие права созданной учетной записи СУБД:

   - 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 предоставить необходимые права созданной учетной записи СУБД, запустите следующий скрипт:

   ```
   /* 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'`.

4. Чтобы просмотреть список привилегий, предоставленных учетной записи СУБД, выполните следующую команду:

   ```
   SHOW предоставляет для 'KSCAdmin'
   ```

5. 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 utf8
   DEFAULT COLLATE utf8_general_ci;
   ```

   Используйте то же имя базы данных, которое вы указали в сценарии, создающем учетную запись СУБД.

6. Установите Сервер администрирования (см. стр. 85).

После завершения установки создается база данных Сервера администрирования и Сервер администрирования готов к работе.

См. также:

Сценарий: Управление программами 588

Настройка учетной записи СУБД для работы с PostgreSQL и Postgres Pro

Предварительные требования

Прежде чем назначать права учетной записи СУБД, 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.

Настройка учетной записи СУБД для установки Сервера администрирования (автоматическое создание базы данных Сервера администрирования)

► *Чтобы настроить учетную запись СУБД 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.

По умолчанию у пользователя *postgres* нет пароля. Но для установки Kaspersky Security Center требуется пароль. Чтобы установить пароль для пользователя *postgres*, запустите следующий скрипт:

```
ALTER USER user_name WITH PASSWORD '<password>';
```

- 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 '<password>' CREATEDB;
  ```

  Созданная роль будет использоваться в качестве владельца базы данных Сервера администрирования (далее также база данных Сервера).

3. Установите Сервер администрирования (см. стр. 85).

После завершения установки автоматически создается база данных Сервера, и Сервер администрирования готов к работе.

Настройка учетной записи СУБД для установки Сервера администрирования (создание базы данных Сервера администрирования вручную)

► *Чтобы настроить учетную запись СУБД 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 '<password>';
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

3. Предоставьте следующие права созданной роли Postgres:

   - Права доступа ко всем таблицам 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. Установите Сервер администрирования (см. стр. 85).

После завершения установки Сервер администрирования будет использовать созданную базу данных для хранения данных Сервера администрирования. Сервер администрирования готов к работе.

kaspersky

Сертификаты для работы с Kaspersky Security Center

В этом разделе содержится информация о сертификатах Kaspersky Security Center и описание, как выпустить и заменить сертификаты для Kaspersky Security Center Web Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с Kaspersky Security Center Web Console.

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;
- Сертификат Веб-сервера
- Сертификат Kaspersky Security Center 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 или в Kaspersky Security Center Web Console 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).

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

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для следующих целей:

- Аутентификация Сервера администрирования при подключении к Kaspersky Security Center Web Console.
- Безопасное взаимодействие Сервера администрирования и Агента администрирования на управляемых устройствах.
- Аутентификация при подключении главных Серверов администрирования к подчиненным Серверам администрирования.

Сертификат Сервера администрирования автоматически создается при установке компонента Сервер администрирования и хранится в папке /var/opt/kaspersky/klnagent_srv/1093/cert/. Сертификат Сервера администрирования вы указываете при создании файла ответов для установки Kaspersky Security Center Web Console (см. стр. 94). Этот сертификат называется общим ("C").

Сертификат Сервера администрирования действителен 397 дней. Kaspersky Security Center автоматически генерирует общий резервный сертификат ("CR") 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.

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

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. 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. 120).

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. стр. 167).

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 указываете мобильный сертификат в свойствах Сервера администрирования.

Также существует мобильный резервный сертификат ("MR"): он используется для замены мобильного сертификата. Kaspersky Security Center автоматически генерирует этот сертификат за 60 дней до истечения срока действия общего 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.

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, в свойствах Сервера администрирования можно указать пользовательские сертификаты, выпущенные другим аккредитованным центром сертификации, при условии, что интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

Сертификат Веб-сервера

Специальный тип сертификата используется Веб-сервером, входящим в состав Сервера администрирования Kaspersky Security Center. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства. Для этого Веб-сервер может использовать различные сертификаты.

Веб-сервер использует один из следующих сертификатов в порядке приоритета:

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Kaspersky Security Center Web Console.
2. Общий сертификат Сервера администрирования ("C").

Сертификат Kaspersky Security Center Web Console

Сервер Kaspersky Security Center 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 может информировать 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. 118) на пользовательский сертификат (рекомендуемый параметр). Создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 116).
- 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 116
Сценарий: Задание пользовательского сертификата Сервера администрирования 120
Начало работы 78
Веб-сервер 54

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. 114).

Таблица 11. Требования для сертификатов Kaspersky Security Center

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • CA: Да. • Ограничение длины пути: Нет Используемые ключи: • Цифровая подпись. • Подпись сертификата. • Шифрование ключей. • Подписывание списка отзыва (CRL). Расширенное использование ключа (Extended Key Usage, EKU) (необязательно): аутентификация Сервера, аутентификация клиента.	Параметр Extended Key Usage является необязательным. Значение ограничения длины пути может быть целым числом отличным от "None", но не меньше 1.
Сертификат Веб-сервера	Расширенное использование ключа (EKU): аутентификация Сервера. Контейнер PKCS #12/PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. 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. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть значение поля `subjectAltName` является допустимым. 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:

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 (см. стр. 118), полученный от аккредитованного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Kaspersky Security Center Web Console.

Когда вы открываете Web Console, браузер может информировать вас о том, что подключение к Web Console не является приватным и что сертификат Web Console недействителен. Это предупреждение появляется потому, что 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. 116).
- 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 перевыпустить просроченный сертификат Kaspersky Security Center Web Console, выполните следующие действия:*

Переустановите Kaspersky Security Center Web Console, выполнив одно из следующих действий:

- Если вы хотите использовать тот же установочный файл Kaspersky Security Center Web Console, удалите Kaspersky Security Center Web Console и установите ту же версию Kaspersky Security Center Web Console (см. стр. 92).
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления (см. стр. 92).

Сертификат Kaspersky Security Center Web Console перевыпущен со сроком действия 397 дней.

Замена сертификата для Kaspersky Security Center Web Console

По умолчанию при установке Сервера Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console Server) сертификат браузера для программы генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

► *Чтобы заменить сертификат для Kaspersky Security Center Web Console на пользовательский сертификат:*

1. Создайте новый файл ответов (см. стр. 94), необходимый для установки Kaspersky Security Center Web Console.
2. В файле ответов укажите путь к файлу пользовательского сертификата и файлу ключа с помощью параметра `CertPath` и параметра `keyPath`.
3. Переустановите Kaspersky Security Center Web Console, указав новый файл ответов. Выполните одно из следующих действий:
   - Если вы хотите использовать тот же установочный файл Kaspersky Security Center Web Console, удалите Kaspersky Security Center Web Console и установите ту же версию Kaspersky Security Center Web Console (см. стр. 92).
   - Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления (см. стр. 92).

Kaspersky Security Center Web Console работает с указанным сертификатом.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center 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 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 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 Web Console (см. стр. 118).

kaspersky

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 ниже.

Тип сертификата: Общий сертификат, общий резервный сертификат ("C", "CR")

Требования:

- Минимальная длина ключа: 2048.
- Основные ограничения:
  - CA: Да.
  - Ограничение длины пути: Нет

    Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
- Используемые ключи:
  - Цифровая подпись.
  - Подпись сертификата.
  - Шифрование ключей.
  - Подписывание списка отзыва (CRL).
- 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.

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:

1. Замена сертификата Сервера администрирования

   Используйте командную строку утилиты klsetsrvcert для этой цели (см. стр. 121).

2. 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. 123).

Результаты

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

См. также:

О сертификатах Kaspersky Security Center 114

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center 116

Начало работы 78

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>`: • `C` – заменить общий сертификат для портов 13000 и 13291. • `CR` – заменить общий резервный сертификат для портов 13000 и 13291.
`-f <time>`	Расписание замены сертификата использует формат "ДД-ММ-ГГГГ ЧЧ:ММ" (для портов 13000 и 13291). Используйте этот параметр, если вы хотите заменить общий или общий резервный сертификат до истечения срока его действия. 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).
`-p <password>`	Пароль, при помощи которого защищен p12-контейнер. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.
`-o <chkopt>`	Параметры проверки сертификата (разделенные точкой с запятой). 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, используйте следующую команду (см. стр. 114):

```
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. 123).

Чтобы не потерять соединения Агентов администрирования, используйте следующую команду:

```
klsetsrvcert -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 120

kaspersky

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

После замены сертификата Сервера администрирования с помощью командной строки утилиты klsetsrvcert вам необходимо установить SSL-соединение между Агентами администрирования и Сервером администрирования, так как соединение разорвано (см. стр. 121).

► *Чтобы указать новый сертификат Сервера 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>]
```

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. В качестве адреса можно указать IP-адрес или DNS-имя.
`-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.

См. также:

Сценарий: Задание пользовательского сертификата Сервера администрирования 120

kaspersky

Задание папки общего доступа

После установки Сервера администрирования можно указать расположение общей папки в свойствах Сервера администрирования. По умолчанию общая папка создается на устройстве с Сервером администрирования. 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.

Вход в программу Kaspersky Security Center Web Console и выход из нее

Вы можете войти в Kaspersky Security Center Web Console после установки Сервера администрирования и Kaspersky Security Center Web Console (см. стр. 81). Вы должны знать веб-адрес Сервера администрирования и номер порта, указанный во время установки (по умолчанию используется порт 8080). В вашем браузере JavaScript должен быть включен.

► *Чтобы войти в Kaspersky Security Center Web Console:*

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 заблокирован.
3. Выполните одно из следующих действий:
   - Для входа на Сервер администрирования:
     a. Введите имя пользователя и пароль внутреннего пользователя или пользователя домена.

        Прежде чем войти в систему с доменной учетной записью пользователя, опросите контроллеры домена, чтобы получить список пользователей домена (см. стр. 178).
     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 **Показать параметры виртуального Сервера**.
     b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера (см. стр. 159).
     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 Web Console и использовать ее для работы с Kaspersky Security Center.

Выход

► *Чтобы выйти из Kaspersky Security Center Web Console,*

В главном меню перейдите в параметры своей учетной записи и выберите **Выйти**.

Программа Kaspersky Security Center Web Console закрыта, отображается страница входа в программу.

kaspersky

Процедура приемки

Перед вводом программы в эксплуатацию проводится процедура приемки, включающая проверку правильной установки, работоспособности и соответствия безопасной (сертифицированной) конфигурации.

В этом разделе

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 (стр. 628).
- Глобальный KSN не используется.

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 14. Шаги алгоритма проверки работоспособности Kaspersky Security Center

Номер шага	Действие	Результат
1	Выполните сценарий развертывания (см. стр. 299) для программ Агент администрирования и Kaspersky Endpoint Security для Linux. Учитывайте, что политику Kaspersky Endpoint Security для Linux вы можете создать как на этом шаге, так и на следующем. В обоих случаях Kaspersky Security Center будет работать корректно.	Установлены Агент администрирования и Kaspersky Endpoint Security для Linux. Управляемые устройства, на которые были установлены эти программы, находятся в группе администрирования, которую вы указали при создании задачи удаленной установки Агента администрирования или автономных инсталляционных пакетов для Агента администрирования. В свойствах устройства, в разделе **Программы**, присутствуют Агент администрирования и Kaspersky Endpoint Security для Linux.
2	Выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки (см. стр. 129).	Мастер первоначальной настройки создал необходимые для управления защитой политики и задачи с параметрами по умолчанию.

Номер шага	Действие	Результат
3	Загрузите обновления в хранилище Сервера администрирования, запустив задачу загрузки обновлений в хранилище (см. стр. 477).	Задача завершена успешно и обновления загружены в хранилище.
4	Внесите произвольные тестовые изменения в политику Kaspersky Endpoint Security для Linux.	Политика применена на управляемом устройстве, обнаруженном в сети: • В свойствах политики присутствует информация о том, что она применена на устройстве. • Параметры программы защиты соответствуют параметрам политики.
5	Скопируйте на одно из управляемых устройств тестовый файл EICAR (см. стр. 557).	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.

Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker

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 утилит klscmodchk и integrity_checker. Утилиты проверяют модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл программы имеет некорректную контрольную сумму, то он считается поврежденным.

Утилита klscmodchk выполняет проверку целостности для следующих компонентов:

- Сервер администрирования
- Агент администрирования

Утилита integrity_checker выполняет проверку целостности для следующих компонентов:

- Сервер администрирования
- Агент администрирования
- Веб-консоль

Обе утилиты проверяют 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 компонента программы содержит файлы, целостность которых важна для корректной работы компонента программы. Целостность самих файлов манифеста также проверяется.

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.

► *Чтобы проверить целостность компонента программы, выполните любую из следующих команд:*

- `$ klscmodchk`

  Утилита klscmodchk запускает программу integrity_checker с нужными параметрами и таким образом проверяет целостность модулей.

- `$ integrity_checker [параметры] <путь к файлу манифеста>`

  Опции программы `integrity_checker`:

  - `--help`: вывести на экран справку утилиты.
  - `--version`: вывести на экран версию утилиты.
  - `--verbose`: вывести на экран информацию о работе утилиты.
  - `--trace <имя файла>`: файл для записи журнала на уровне DEBUG.
  - `--signature-type <dskm2 | kds | kds-with-filename>`: тип проверяемой сигнатуры, по умолчанию dskm2.
  - `--crl <директория>`: путь к директории, которая содержит отозванные сертификаты и подписи (CRL) для KDS. Значение игнорируется, если директория не существует или пуста.

Результат проверки каждого файла манифеста выводится рядом с названием файла манифеста в следующем виде:

- SUCCEEDED – целостность файлов подтверждена (код возврата 0).
- FAILED – целостность файлов не подтверждена (код возврата не 0).

Рекомендуется запускать утилиту проверки целостности с сертифицированного компакт-диска, чтобы гарантировать целостность утилиты. При запуске с компакт-диска требуется указать полный путь к файлу манифеста в папке программы.

kaspersky

Мастер первоначальной настройки

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 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 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 вы хотите 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 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:

- **Область**

  Вы можете выбрать одну из следующих областей защиты:

  - **Рабочие станции.**
  - **Файловые серверы и системы хранения данных.**
  - **Виртуальные среды.**
  - **Банкоматы и POS-системы.**
  - **Промышленные сети.**
  - **Промышленные конечные точки.**

- **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 Web Console.

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 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:

- Быстрое шифрование. Для этого типа шифрования используется 56-разрядный ключ.
- Стойкое шифрование. Для этого типа шифрования используется 256-разрядный ключ.

Вы можете выбрать дистрибутив для Kaspersky Endpoint Security для Windows с требуемым 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 столбцы:

- **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 или**.

После выбора подключаемых модулей нажмите на кнопку **Далее**, чтобы начать установку.

Вы можете установить плагины управления для программ "Лаборатории Касперского" 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.

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 программы для языка Kaspersky Security Center отсутствует, 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.

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. 399). 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) позднее без запуска мастера первоначальной настройки (см. стр. 400).

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 разделе **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"** главного меню.

- 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 разделе **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"** главного меню.

- Отложите активацию программы

Если вы отложили активацию программы, вы можете добавить 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.

Шаг 9. 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.

Шаг 10. 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:

- **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.

- **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
  - 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.

Вы можете проверить установленные параметры отправки почтовых уведомлений с помощью кнопки **Отправить пробное сообщение**.

kaspersky

Шаг 11. Завершение работы мастера первоначальной настройки

Для завершения работы мастера нажмите на кнопку **Готово**.

После завершения работы мастера первоначальной настройки вы можете запустить мастер развертывания защиты для автоматической установки программ безопасности или Агента администрирования на устройства в вашей сети (см. стр. 136).

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 находится в узле **Опрос 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. 315) и настройте Агент администрирования.

kaspersky

См. также:

В этом разделе

Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

► *Чтобы запустить мастер развертывания защиты вручную,*

В главном окне программы перейдите в раздел **Опрос и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

Запустится мастер развертывания защиты. Для продолжения работы мастера нажмите на кнопку **Далее**.

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:

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;
  - 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 136

Сценарий: Развертывание программ "Лаборатории Касперского" 299

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.

- **Выбрать устройства 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 136
Сценарий: Развертывание программ "Лаборатории Касперского" 299

Шаг 5. Задание параметров задачи удаленной установки

На странице **Параметры 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 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.

  Единственный способ установить программу для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке программы для Windows:

  - Выберите этот параметр.
  - Убедитесь, что для целевых клиентских устройств назначена точка распространения.
  - Убедитесь, что на точке распространения установлена операционная система Windows.

- 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 дополнительный параметр:

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.

Шаг 6. 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.

Шаг 7. 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.

Шаг 8. 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 (Агент администрирования не используется)**

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.

Шаг 9. 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.

kaspersky

Обновление предыдущей версии Kaspersky Security Center

Вы можете установить Сервер администрирования версии 15 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 13). При обновлении до версии 15 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Во время обновления недопустимо совместное использование СУБД Сервером администрирования и какой-либо другой программой.

Вы можете обновить версию Сервера администрирования одним из следующих способов:

- С помощью установочного файла Kaspersky Security Center (см. стр. 142).
- Создав резервную копию данных Сервера администрирования, установив новую версию Сервера администрирования и восстановив данных Сервера администрирования из резервной копии (см. стр. 144).

Если в вашей сети несколько Серверов администрирования, вам необходимо обновить каждый Сервер вручную. Kaspersky Security Center не поддерживает централизованное обновление.

При обновлении предыдущей версии Kaspersky Security Center все установленные плагины поддерживаемых программ "Лаборатории Касперского" сохраняются. Плагины Сервера администрирования и Агента администрирования обновляются автоматически.

В этом разделе

Обновление предыдущей версии Kaspersky Security Center с помощью файла установки

Для обновления Сервера администрирования с предыдущей версии (начиная с версии 13) до версии 15 вы можете установить новую версию поверх предыдущей с помощью установочного файла Kaspersky Security Center.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 15 с помощью установочного файла:*

1. Загрузите установочный файл Kaspersky Security Center с полным пакетом для версии 15 с сайта "Лаборатории Касперского":

- Для устройств с операционной системой на базе RPM: ksc64-<номер версии>-11247.x86_64.rpm.
- Для устройств с операционной системой на основе Debian: ksc64_<номер версии>-11247_amd64.deb.

2. Обновите инсталляционный пакет с помощью диспетчера пакетов, который вы используете на своем Сервере администрирования. Например, вы можете использовать следующие команды в терминале командной строки под учетной записью с привилегиями root:

   - Для устройств с операционной системой на основе RPM:

   ```
   $ sudo rpm -Uvh --nodeps --force ksc64-<номер версии>-11247.x86_64.rpm
   ```

   - Для устройств с операционной системой на основе Debian:

   ```
   $ sudo dpkg -i ksc64_<номер версии>-11247_amd64.deb
   ```

   После успешного выполнения команды создается скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Сообщение об этом отображается в терминале.

3. Запустите скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl для настройки обновленного Сервера администрирования.

4. Прочтите Лицензионное соглашение и Политику конфиденциальности, которые отображаются в терминале командной строки. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности:

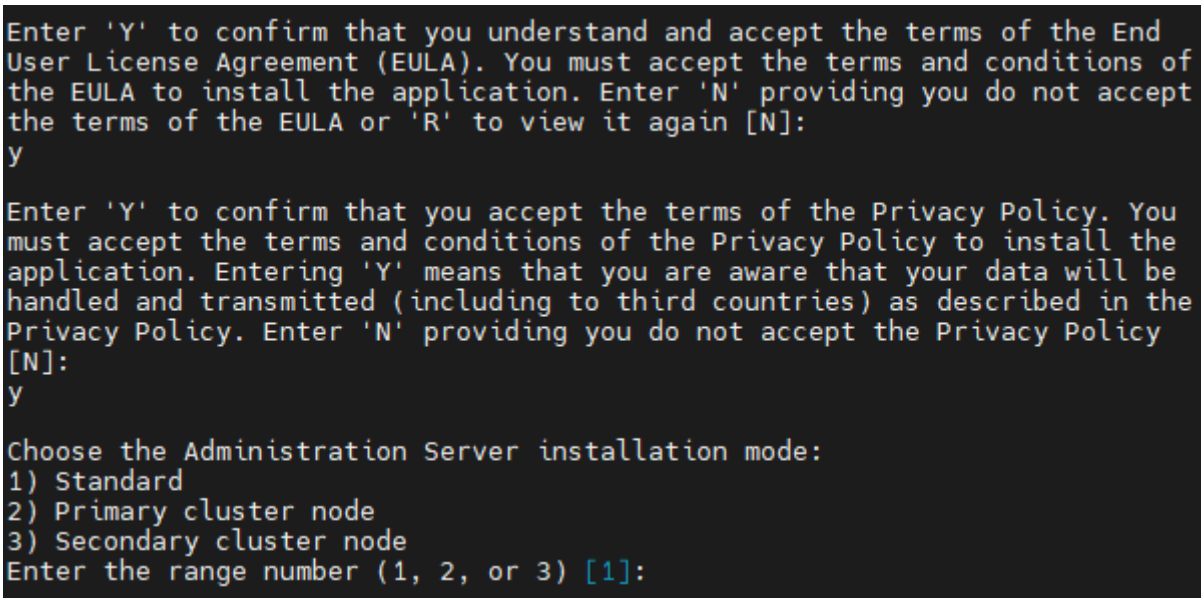
   a. Введите "Y", чтобы подтвердить, что вы полностью прочитали, поняли и принимаете положения и условия Лицензионного соглашения.

   b. Введите "Y" еще раз, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете Политику конфиденциальности, описывающую обработку данных.

   Установка программы будет продолжена после того, как вы дважды введете "Y".

5. Введите "1", чтобы выбрать стандартный режим установки Сервера администрирования.

   На картинке ниже показаны последние два шага.



   Далее скрипт настраивает и завершает обновление Сервера администрирования. Во время обновления вы не можете изменить параметры Сервера администрирования, которые были изменены до обновления.

6. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования.

   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 предыдущей версии Kaspersky Security Center с помощью резервной копии 144

Обновление предыдущей версии Kaspersky Security Center с помощью резервной копии

Для обновления Сервера администрирования с предыдущей версии (начиная с версии 13) до версии 15 вы можете создать резервную копию данных Сервера администрирования и восстановить эти данные после установки Kaspersky Security Center новой версии. Если при установке возникли проблемы, вы можете восстановить предыдущую версию Сервера администрирования, используя созданную перед обновлением резервную копию данных Сервера.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 15 с помощью резервной копии данных:*

1. Перед обновлением, выполните резервное копирование данных Сервера администрирования старой версии программы (см. стр. 167).
2. Удалите старую версию Kaspersky Security Center.
3. Установите Kaspersky Security Center версии 15 на бывшем Сервере администрирования (см. стр. 78).
4. Восстановите данные Сервера администрирования из резервной копии данных, созданной перед обновлением (см. стр. 167).
5. Для устройств, на которых был установлен Агент администрирования предыдущей версии, создайте и запустите задачу удаленной установки новой версии Агента администрирования.

   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 предыдущей версии Kaspersky Security Center с помощью файла установки.....142

kaspersky

Обновление Kaspersky Security Center на узле отказоустойчивого кластера "Лаборатории Касперского"

Вы можете установить Сервер администрирования версии 15 на каждый узел отказоустойчивого кластера "Лаборатории Касперского", где установлен Сервер администрирования более ранней версии (начиная с версии 14). При обновлении до версии 15 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Если вы ранее установили Kaspersky Security Center на устройства локально, также можно обновить Kaspersky Security Center на этих устройствах с помощью установочного файла (см. стр. 142) или с помощью резервной копии (см. стр. 144).

► *Чтобы обновить Kaspersky Security Center на узле отказоустойчивого кластера "Лаборатории Касперского":*

1. Загрузите установочный файл Kaspersky Security Center с полным пакетом для версии 15 с сайта "Лаборатории Касперского":
   - Для устройств с операционной системой на базе RPM: ksc64-<номер версии>-<номер сборки>.x86_64.rpm.
   - Для устройств с операционной системой на основе Debian: ksc64_<номер версии>-<номер сборки>_amd64.deb.
2. Остановить кластер (см. стр. 108).
3. Обновите инсталляционный пакет на активном узле кластера с помощью диспетчера пакетов, который вы используете на своем Сервере администрирования.

   Например, вы можете использовать следующие команды в терминале командной строки под учетной записью с привилегиями root:
   - Для устройств с операционной системой на основе RPM:

     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<номер версии>-<номер сборки>.x86_64.rpm
     ```
   - Для устройств с операционной системой на основе Debian:

     ```
     $ sudo dpkg -i ksc64_<номер версии>-<номер сборки>_amd64.deb
     ```

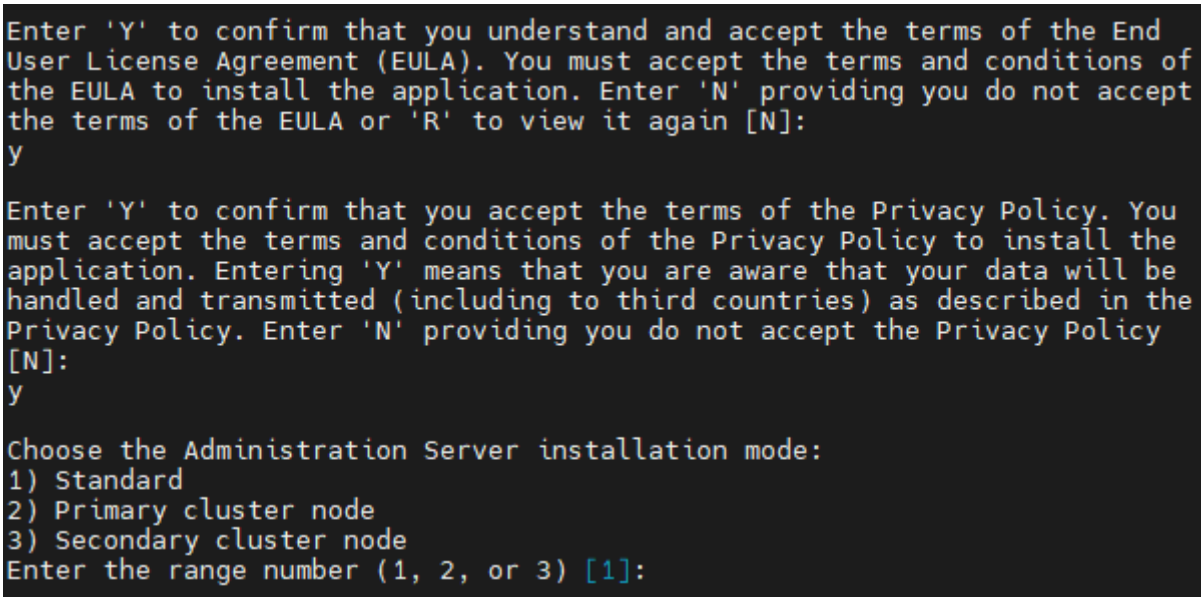
   После успешного выполнения команды создается скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Сообщение об этом отображается в терминале.
4. Запустите скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl для настройки обновленного Сервера администрирования.
5. Прочтите Лицензионное соглашение и Политику конфиденциальности, которые отображаются в терминале командной строки. Если вы согласны со всеми условиями Лицензионного соглашения и Политики конфиденциальности:
   a. Введите "Y", чтобы подтвердить, что вы полностью прочитали, поняли и принимаете положения и условия Лицензионного соглашения.

b. Введите "Y" еще раз, чтобы подтвердить, что вы полностью прочитали, поняли и принимаете Политику конфиденциальности, описывающую обработку данных.

Установка программы будет продолжена после того, как вы дважды введете "Y".

6. Выберите узел, на котором вы выполняете обновление, указав "2".

На картинке ниже показаны последние два шага.



Далее скрипт настраивает и завершает обновление Сервера администрирования. Во время обновления вы не можете изменить параметры Сервера администрирования, которые были изменены до обновления.

7. Выполните шаги 3–5 на пассивном узле.

На шаге 6 введите "3", чтобы выбрать узел.

8. Запустить кластер (см. стр. 108).

> Обратите внимание, вы можете запустить кластер на любом узле. Если вы запускаете кластер на пассивном узле, он становится активным узлом.

В результате вы установили Сервер администрирования последней версии на узлы отказоустойчивого кластера "Лаборатории Касперского".

kaspersky

Перенос данных в программу Kaspersky Security Center

В этом разделе представлена информация о способах переноса данных из программы Kaspersky Security Center Windows в Kaspersky Security Center.

С помощью функции переноса данных вы можете перенести структуру группы администрирования, входящие в нее управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky Security Center.

Для переноса всех объектов используйте мастер переноса данных. Этот мастер сохраняет выбранные объекты в ZIP-файл (см. стр. 148) и позволяет импортировать эти объекты из ZIP-файла в Kaspersky Security Center (см. стр. 149). Помимо мастера, вы также можете передавать выбранные политики и задачи с помощью файлов KLP и KLT.

Чтобы завершить перенос данных и переключить импортированные управляемые устройства под управление Kaspersky Security Center, в текущей версии Kaspersky Security Center вы можете выполнить одно из следующих действий:

- Использовать утилиту klmover (см. стр. 123).
- Указать параметры подключения Сервера администрирования Kaspersky Security Center в свойствах инсталляционного пакета Агента администрирования и использовать этот инсталляционный пакет для установки Агента администрирования на импортированные управляемые устройства с помощью задачи удаленной установки (см. стр. 316).

  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. 258) и включите параметр **Средствами операционной системы с помощью точек распространения** в задаче удаленной установки. Подробнее см. в разделе Переключение управляемых устройств под управление Kaspersky Security Center (см. стр. 150).

Вы можете перенести управляемые устройства и данные в Kaspersky Security Center следующими способами:

- Перенесите управляемые устройства и данные с помощью мастера переноса данных (см. стр. 148):
  - Перенос данных без иерархии Серверов администрирования

    Выберите этот параметр, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center не выстроены в иерархию. Вы будете управлять процессом переноса данных с помощью двух экземпляров Kaspersky Security Center Web Console – одного экземпляра Kaspersky Security Center Windows и одного экземпляра Kaspersky Security Center. В этом случае вы будете использовать файл экспорта (ZIP-архив), который вы создали и загрузили во время экспорта из Kaspersky Security Center Windows (см. стр. 148), и импортировать этот файл в Kaspersky Security Center (см. стр. 149).
  - 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. Вы будете управлять процессом переноса данных и переключатся между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console для Kaspersky Security Center. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в

иерархию, чтобы упростить процедуру переноса данных. Для этого создайте иерархию перед началом переноса данных.

- Экспортируйте определенные задачи (см. стр. 416) из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky Security Center (см. стр. 416).
- Экспортируйте определенные политики (см. стр. 372) из Kaspersky Security Center Windows, а затем импортируйте политики в Kaspersky Security Center (см. стр. 372). Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

В этом разделе

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, включающей в себя управляемые устройства и другие объекты группы из Kaspersky Security Center Windows в Kaspersky Security Center, вам нужно предварительно выбрать данные для экспорта и создать файл экспорта. Файл экспорта содержит информацию обо всех групповых объектах, которые вы хотите перенести. Файл экспорта будет использоваться для последующего импорта в Kaspersky Security Center.

Вы можете экспортировать следующие объекты:

- Задачи и политики управляемых программ.
- Глобальные задачи (см. стр. 406)
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите (см. стр. 285).

Перед началом экспорта прочтите общую информация о переносе данных в Kaspersky Security Center (см. стр. 147). Выберите способ переноса данных: с использованием или без использования иерархии Серверов администрирования Kaspersky Security Center Windows и Kaspersky Security Center.

► *Чтобы экспортировать управляемые устройства и связанные объекты группы с помощью мастера переноса данных:*

1. В зависимости от того, выстроены ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center, выполните одно из следующих действий:
   - Если Серверы выстроены в иерархию, откройте Kaspersky Security Center Web Console и переключитесь на Сервер администрирования Kaspersky Security Center Windows.
   - Если Серверы не выстроены в иерархию, откройте Kaspersky Security Center Web Console, подключенную к Kaspersky Security Center Windows.
2. В главном окне программы перейдите в раздел **Операции** → **Перенос данных**.

3. Выберите **Перенести данные в Kaspersky Security Center**, 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. 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.

Файл экспорта (ZIP-архив) создан. В зависимости от того, выполняете ли вы перенос данных с поддержкой иерархии Сервера администрирования, файл экспорта сохраняется следующим образом:

- Если Серверы выстроены в иерархию, файл экспорта сохраняется во временную папку на Сервере Kaspersky Security Center Web Console.
- Если Серверы не организованы в иерархию, файл экспорта загружается на ваше устройство.

Для переноса данных с поддержкой иерархии Сервера администрирования импорт начинается автоматически после успешного экспорта (см. стр. 150). Для переноса данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky Security Center (см. стр. 150).

Импорт экспортного файла в Kaspersky Security Center

Чтобы передать информацию об управляемых устройствах, объектах и их параметрах, которые вы экспортировали из Kaspersky Security Center Windows, вам нужно импортировать ее в программу Kaspersky Security Center (см. стр. 148).

► *Чтобы импортировать управляемые устройства и связанные объекты группы с помощью мастера переноса данных:*

1. В зависимости от того, выстроены ли в иерархию Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center, выполните одно из следующих действий:
   - Если Серверы выстроены в иерархию, переходите к следующему шагу мастера переноса данных после завершения экспорта. Импорт начнется автоматически после успешного экспорта в этом мастере (см. шаг 2 этой инструкции) (см. стр. 148).
   - Если Серверы не выстроены в иерархию:
     a. Откройте Kaspersky Security Center Web Console, подключенный к Kaspersky Security Center.
     b. В главном окне программы перейдите в раздел **Операции → Перенос данных**.
     c. Выберите файл экспорта (ZIP-архив), который вы создали и загрузили при экспорте из Kaspersky Security Center Windows (см. стр. 148). Начнется загрузка файла экспорта.
2. После успешной загрузки файла экспорта вы можете продолжить импорт. Если вы хотите указать другой файл для экспорта, перейдите по ссылке **Изменить** и выберите нужный файл.
3. Отобразится вся иерархия групп администрирования Kaspersky Security Center.

Установите флажок рядом с целевой группой администрирования, в которой необходимо восстановить объекты экспортированной группы администрирования (управляемые устройства, политики, задачи и другие объекты группы).

4. Начнется импорт объектов группы. Свернуть мастер переноса данных и выполнять любые параллельные операции во время импорта нельзя. Дождитесь, пока значки () рядом со всеми пунктами в списке объектов заменятся на зеленые флажки () и импорт завершится.
5. Когда импорт завершится, экспортированная структура групп администрирования, включая сведения об устройствах, появится в целевой группе администрирования, которую вы выбрали. Если имя восстанавливаемого объекта совпадает с именем существующего объекта, к восстановленному будет добавлен дополнительный суффикс.

Если импорт завершился с ошибкой, вы можете выполнить одно из следующих действий:

- Для переноса данных с поддержкой иерархии Сервера администрирования вы можете импортировать файл экспорта еще раз.
- Для переноса данных без поддержки иерархии Сервера администрирования вы можете запустить мастер переноса данных, чтобы выбрать другой файл экспорта, а затем импортировать его снова.

Вы можете проверить, были ли объекты группы, входящие в область экспорта, успешно импортированы в Kaspersky Security Center. Для этого перейдите в раздел **Активы (Устройства)** и убедитесь, что импортированные объекты отображаются в соответствующих подразделах.

Обратите внимание, что импортированные управляемые устройства отображаются в подразделе **Управляемые устройства**, но они не видны в сети и на них не установлен и не запущен Агент администрирования (значение *Нет* в столбцах **Видимый**, **Агент администрирования установлен**, **Агент администрирования работает**).

Для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center (см. стр. 150).

Переключение управляемых устройств под управление Kaspersky Security Center

После успешного импорта информации об управляемых устройствах, объектах и их параметрах в Kaspersky Security Center для завершения переноса данных вам необходимо переключить управляемые устройства под управление Kaspersky Security Center.

В текущей версии Kaspersky Security Center вы можете переместить управляемые устройства под управление Kaspersky Security Center либо с помощью утилиты klmover (см. стр. 123), либо установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки (см. стр. 316).

► *Чтобы переключить управляемые устройства под управление Kaspersky Security Center, установив Агент администрирования:*

1. Переключитесь на Сервер администрирования Kaspersky Security Center Windows.
2. Перейдите в раздел **Обнаружение и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты** и откройте свойства существующего инсталляционного пакета Агента администрирования (см. стр. 234).

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый (см. стр. 302).

3. На закладке **Общие** выберите раздел **Порты подключения**. Укажите параметры подключения Сервера администрирования Kaspersky Security Center.
4. Создайте задачу удаленной установки для импортированных управляемых устройств, а затем укажите перенастроенный инсталляционный пакет Агента администрирования (см. стр. 316).

   Вы можете установить Агент администрирования с помощью Сервера администрирования Kaspersky Security Center Windows или с помощью устройства под управлением Windows, которое выполняет роль точки распространения (см. стр. 258). Если вы используете Сервер администрирования, включите параметр **Средствами операционной системы с помощью Сервера администрирования**. Если вы используете точку распространения, включите параметр **Средствами операционной системы с помощью точки распространения**.
5. Запустите задачу удаленной установки программы.

После успешного завершения задачи удаленной установки перейдите на Сервер администрирования Kaspersky Security Center и убедитесь, что управляемые устройства видны в сети и что на них установлен и запущен Агент администрирования (значение *Да* в столбцах **Видимо**, **Агент администрирования установлен** и **Агент администрирования запущен**).

kaspersky

Настройка Сервера администрирования

В этом разделе описан процесс настройки и свойства Сервера администрирования Kaspersky Security Center.

В этом разделе

Настройка параметров подключения Kaspersky Security Center 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.

kaspersky

См. также:

Порты, используемые Kaspersky Security Center.....45

Настройка списка разрешенных IP-адресов для входа в Kaspersky Security Center

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором они могут открыть Kaspersky Security Center Web Console. 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 604). 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. 531) 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 Kaspersky Security Center через Kaspersky Security Center Web Console, вы можете настроить сетевой экран на устройстве, где установлен Сервер Kaspersky Security Center Web Console, штатными средствами операционной системы. Затем, если кто-то попытается войти в Kaspersky Security Center на одном устройстве, а Сервер Kaspersky Security Center Web Console установлен на другом устройстве (см. стр. 45), сетевой экран поможет предотвратить вмешательство злоумышленников.

- 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 папку на папку установки Kaspersky Security Center (обычно это /opt/kaspersky/ksc64/sbin).
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 Syslog 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.

kaspersky

Иерархия Серверов администрирования

Некоторые компании-клиенты, например MSP-клиенты, могут использовать несколько Серверов администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию. Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

Взаимодействие "главный – подчиненный" между двумя Серверами администрирования предоставляет следующие возможности:

- Подчиненный Сервер наследует с главного Сервера политики, задачи, роли пользователей и инсталляционные пакеты, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты и выборки событий на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.
- Главный Сервер администрирования может использоваться в качестве источника обновлений для подчиненного Сервера администрирования.

Создание иерархии Серверов администрирования: добавление подчиненного Сервера администрирования

Сервер администрирования с операционной системой Linux может работать в иерархии Серверов как в качестве главного Сервера, так и в качестве подчиненного Сервера. Главный Сервер с операционной системой Linux может управлять подчиненными Серверами с операционными системами и Linux и Windows. Главный Сервер с операционной системой Windows может управлять подчиненным Сервером с операционной системой Linux.

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 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 нажмите на 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:

   - **Отображаемое 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 (если требуется)**

     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.

   - **Использовать прокси-сервер**

     Выберите этот параметр, если вы используете прокси-сервер для подключения подчиненного Сервера администрирования.

     В этом случае вы также можете указать следующие параметры прокси-сервера:

     - **Адрес.**
     - **Имя пользователя.**
     - **Пароль**

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 вы можете создать иерархию только из будущего подчиненного Сервера (см. инструкции ниже). Это известная ошибка (см. стр. 613).

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 вручную.

Соединение также может завершиться ошибкой 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 создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам (см. стр. 116).
- Добавить самоподписанный сертификат будущего подчиненного Сервера 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.

После завершения работы мастера иерархия "главный Сервер – подчиненный Сервер" создана. 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, недоступен или потому что файл сертификата подчиненного Сервера администрирования является самоподписанным), вы все равно можете добавить подчиненный Сервер администрирования.

► *Чтобы добавить Сервер администрирования, недоступный для подключения через Kaspersky Security Center 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, /var/opt/kaspersky/klnagent_srv/1093/cert/.

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, установите флажок **Использовать прокси-сервер** и задайте 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:

Порты, используемые Kaspersky Security Center.....45

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 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.
- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер (см. стр. 155). После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.

kaspersky

Управление виртуальными Серверами администрирования

В этом разделе описываются следующие действия, как управлять виртуальными Серверами администрирования:

- создание виртуальных Серверов администрирования (см. стр. 159);
- включение и выключение виртуальных Серверов администрирования (см. стр. 160);
- назначение администратора виртуального Сервера администрирования (см. стр. 160);
- смена Сервера администрирования для клиентских устройств (см. стр. 162);
- удаление виртуальных Серверов администрирования (см. стр. 164).

В этом разделе

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования (см. стр. 205).

► *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 **Серверы 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 **Новый 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 **Серверы 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 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center Web Console.
- Используйте Kaspersky Security Center Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер (см. стр. 155). После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.

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 **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите включить или выключить.
4. В меню нажмите на кнопку **Включение и выключение виртуального Сервера 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 164

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, администратор виртуального Сервера администрирования указывает имя виртуального Сервера администрирования, имя пользователя и пароль (см. стр. 124). Kaspersky Security Center 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. 159).
- На главном Сервере администрирования у вас создана учетная запись для администратора, которого вы хотите назначить для виртуального Сервера администрирования.
- У вас есть право И**зменения списков управления доступом к объектам** (см. стр. 432) в функциональной области **Общие функции** → **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 именом Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **Правила доступа** 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 **OK**.

   Программа добавляет выбранного пользователя в список пользователей на вкладку **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:

   - **Чтение** в функциональной области **Общий функционал** → **Базовая функциональность**.
   - **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 и укажите все необходимые права доступа, которыми должен обладать администратор на виртуальном Сервере администрирования (см. стр. 464). 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. 450).

   Программа назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области (см. стр. 432), вы можете настроить доступ к определенным объектам (см. стр. 444) 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 164

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 **Активы (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.
   - **Укажите 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 в соответствии с вашими требованиями (см. стр. 410).
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 159
Сценарий: Настройка защиты сети 349

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 Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Серверы администрирования**.
3. Выберите виртуальный Сервер администрирования, который вы хотите удалить.
4. В меню выберите пункт **Удалить**.

Виртуальный Сервер администрирования удален.

См. также:

Включение и выключение виртуального Сервера администрирования 160

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 событий**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

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 – 400000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Программа проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 00 больше указанного максимального значения, программа удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

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 **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **Сохранить**.

См. также:

О блокировке частых событий 543

Сценарий: Настройка защиты сети 349

kaspersky

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. 168) с помощью Kaspersky Security Center Web Console или запустите утилиту klbackup (см. стр. 169).

2. Выберите новое устройство, на которое будет установлен Сервер администрирования. Убедитесь, что аппаратное и программное обеспечение на выбранном устройстве соответствует требованиям для Сервера администрирования, Kaspersky Security Center Web Console и Агента администрирования (см. стр. 18). Проверьте, что порты, используемые на Сервере администрирования доступны (см. стр. 45).

3. На новом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования (см. стр. 81).

   При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.

4. Установите Сервер администрирования на новое устройство.

   Обратите внимание, что если вы переносите сервер базы данных на новое устройство, вам требуется указать локальный адрес в качестве IP-адреса устройства, на котором установлена база данных (пункт "h" инструкции Установка Kaspersky Security Center) (см. стр. 85). Если вам нужно сохранить сервер базы данных на предыдущем устройстве, введите IP-адрес предыдущего устройства в пункте "h" инструкции Установка Kaspersky Security Center (см. стр. 85).

5. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.

   > 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.

6. Откройте Kaspersky Security Center Web Console и подключитесь к Серверу администрирования (см. стр. 124).

7. Убедитесь, что все клиентские устройства подключены к Серверу администрирования.

8. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

kaspersky

См. также:

Смена Сервера администрирования для клиентских устройств.....296
Резервное копирование и восстановление данных Сервера администрирования.....167

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 Linux с помощью утилиты klsrvconfig:*

1. Запустите командную строку Linux.
2. В открывшемся окне командной строки утилиты klsrvconfig укажите:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```
3. Укажите новое имя учетной записи. Вы должны указать учетные данные учетной записи, которая существует в СУБД.
4. Введите новый пароль.
5. Укажите этот новый пароль для подтверждения.

Учетные данные СУБД изменены.

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 через Kaspersky Security Center Web Console (см. стр. 168).
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования (см. стр. 169). Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки

Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы (обычно, /opt/kaspersky/ksc64/sbin/klbackup).

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.

См. также:

Обновление предыдущей версии Kaspersky Security Center с помощью резервной копии 144

В этом разделе

Создание задачи резервного копирования данных Сервера администрирования 168

Использование утилиты klbackup для резервного копирования и восстановления данных 169

Создание задачи резервного копирования данных Сервера администрирования

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки (см. стр. 129). Если задача резервного копирования, созданная мастером первоначальной настройки, была удалена, вы можете создать ее вручную.

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.

► *Чтобы создать задачу резервного копирования данных Сервера администрирования:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. На первой странице мастера в списке **Программа** выберите **Kaspersky Security Center 15** и в списке **Тип задачи** выберите **Резервное копирование данных Сервера администрирования**.
4. На соответствующей странице мастера укажите следующую информацию:

- папку для хранения резервных копий;
- пароль для резервной копии (не обязательно);
- максимальное количество сохраненных резервных копий.

5. 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.
6. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Использование утилиты klbackup для резервного копирования и восстановления данных

Вы можете выполнять копирование данных Сервера администрирования для резервного хранения и последующего восстановления с помощью утилиты klbackup, входящей в состав дистрибутива Kaspersky Security Center.

► *Чтобы создать резервную копию данных или восстановить данные Сервера администрирования в тихом 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.

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.

kaspersky

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
```

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center Web Console на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

► *Чтобы настроить интерфейс Kaspersky Security Center 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 параметр **Показать раздел "Шифрование и защита данных"**.
3. Нажмите на кнопку **Сохранить**.

   После этого в главном меню появится раздел **Операции → Шифрование и защита данных**.

Шифрование подключения TLS

Чтобы закрыть уязвимости в сети вашей организации, вы можете включить шифрование трафика с использованием TLS-протокола. Вы можете включить протоколы шифрования TLS и поддерживаемые наборы шифров на Сервере администрирования. Kaspersky Security Center поддерживает TLS-протокол версий 1.0, 1.1, 1.2 и 1.3. Вы можете выбрать требуемый протокол шифрования и наборы шифрования.

Kaspersky Security Center использует самоподписанные сертификаты. Также вы можете использовать ваши собственные сертификаты. Рекомендуется использовать сертификаты, подписанные аккредитованным центром сертификации.

► *Чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования:*

1. Запустите утилиту klscflag.

   Утилита klscflag находится в папке, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

2. Используйте флаг SrvUseStrictSslSettings, чтобы настроить разрешенные протоколы шифрования и наборы шифрования на Сервере администрирования. Выполните следующую команду в командной строке, используя учетную запись с правами администратора:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUse-
   StrictSslSettings -v <value> -t d
   ```

   Укажите параметр <value> флага SrvUseStrictSslSettings:

   - `4` – включены только TLS-протоколы версий 1.2 и 1.3. Также включены наборы шифрования с TLS_RSA_WITH_AES_256_GCM_SHA384 (эти наборы шифрования необходимы для обратной совместимости с Kaspersky Security Center 11). Это значение по умолчанию.

     Наборы шифрования поддерживают TLS-протокол 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (с набором шифрования TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Наборы шифрования поддерживают TLS-протокол 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` – включены только TLS-протоколы версий 1.2 и 1.3. Для TLS-протоколов версий 1.2 и 1.3 поддерживаются определенные наборы шифрования, перечисленные ниже.

     Наборы шифрования поддерживают TLS-протокол 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Наборы шифрования поддерживают TLS-протокол 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Не рекомендуется использовать значения 0, 1, 2 или 3 для значений параметра флага SrvUseStrictSslSettings. Эти значения параметров соответствуют небезопасным версиям TLS-протокола (TLS 1.0 и TLS 1.1) и небезопасным наборам шифрования и используются только для обратной совместимости с более ранними версиями Kaspersky Security Center.

3. Перезапустите следующие службы Kaspersky Security Center:
   - Сервер администрирования
   - Веб-сервер
   - службу активации прокси-сервера.

В результате включается шифрование трафика с помощью TLS-протокола.

Вы можете использовать флаги KLTR_TLS12_ENABLED и KLTR_TLS13_ENABLED, чтобы включить поддержку TLS-протоколов 1.2 и 1.3 соответственно. Эти флаги включены по умолчанию.

► *Чтобы включить или выключить поддержку TLS-протоколов 1.2 и 1.3:*

1. Запустите утилиту klscflag.

   Утилита klscflag находится в папке, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

2. Выполните одну из команд в командной строке, используя учетную запись с правами администратора:
   - Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.2:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n
     KLTR_TLS12_ENABLED -v <value> -t d
     ```

   - Используйте эту команду, чтобы включить или выключить поддержку TLS-протокола 1.3:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n
     KLTR_TLS13_ENABLED -v <value> -t d
     ```

   Укажите параметр <value> флага:

   - `1` – чтобы включить поддержку TLS-протокола.
   - `0` – чтобы выключить поддержку TLS-протокола.

kaspersky

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:

- управляемые 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. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

Обнаружение сетевых устройств состоит из следующих этапов:

1. Первоначальное обнаружение устройств

   После завершения работы мастера первоначальной настройки, выполните опрос сети для обнаружения устройств вручную.

a. Настройка будущих опросов

Убедитесь, что опрос IP-диапазонов (см. стр. 175) включен и что расписание опроса соответствует требованиям вашей организации. При настройке расписания опроса опирайтесь на рекомендации для частоты опросов сети.

Также можно включить опрос Zeroconf (см. стр. 178), если в вашей сети есть IPv6-устройства.

Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена (см. стр. 178).

b. **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**. При необходимости можно настроить правила автоматического перемещения этих устройств (см. стр. 244) в группу **Управляемые устройства**. Можно также настроить правила хранения.

Если вы пропустили этап, на котором задаются правила, все новые обнаруженные устройства будут помещены в группу **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**.

Опрос IP-диапазонов

Kaspersky Security Center пытается выполнить обратное преобразование имен: для каждого IPv4-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. Если эта зона не настроена, опрос IP-подсети не даст результатов.

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.

Если включен только опрос IP-диапазонов, Kaspersky Security Center обнаруживает устройства только с IPv4-адресами. Если в вашей сети есть IPv6-устройства, включите опрос Zeroconf (см. стр. 178) устройств.

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. 177). 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:

   - **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 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**.

kaspersky

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. 178), 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. 175). 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**. 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.

Опрос Zeroconf

Этот тип опроса поддерживается только для точек распространения с операционными системами Linux.

Kaspersky Security Center может опрашивать сети, в которых есть устройства с IPv6-адресами. В этом случае IP-диапазоны не указываются, и Kaspersky Security Center опрашивает всю сеть, используя сеть с нулевой конфигурацией http://www.zeroconf.org/ (далее также *Zeroconf*). Чтобы начать использовать Zeroconf, необходимо установить утилиту avahi-browse на устройство с операционной системой Linux, которое опрашивает сети, то есть на Сервер администрирования или на точку распространения.

► *Чтобы включить опрос Zeroconf:*

1. В главном окне 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 Kaspersky Security Center начинает опрашивать вашу сеть. В этом случае указанные IP-диапазоны игнорируются.

Опрос контроллеров домена

Kaspersky Security Center поддерживает опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba. Для контроллеров домена Samba, в качестве контроллеров домена Active Directory используется Samba 4 (см. стр. 181).

При опросе контроллера домена Сервер администрирования или точка распространения получают информацию о структуре домена, учетных записях пользователей, группах безопасности и о DNS-именах устройств, входящих в домен.

Рекомендуется использовать опрос контроллеров домена, если все сетевые устройства являются членами домена. Если некоторые из сетевых устройств не включены в домен, эти устройства не могут быть обнаружены с помощью опроса контроллеров домена.

Предварительные требования

Перед опросом контроллеров домена убедитесь, что включены следующие протоколы:

- Simple Authentication and Security Layer (SASL).
- Lightweight Directory Access Protocol (LDAP).

Убедитесь, что на устройстве контроллеров домена доступны следующие порты:

- 389 для SASL.
- 636 для TLS.

Опрос контроллеров домена с помощью Сервера администрирования

► *Чтобы опросить контроллеры домена с помощью Сервера администрирования:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.
2. Нажмите на кнопку **Параметры опроса**.

   Откроется окно **Параметры опроса контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. В разделе **Опрос указанных доменов** нажмите на кнопку **Добавить**, укажите адрес и учетные данные пользователя контроллеров домена.
5. При необходимости в окне **Параметры опроса контроллеров домена** укажите расписание 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 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.

Если вы измените учетные записи пользователей в группе безопасности домена, эти изменения отобразятся в Kaspersky Security Center через час после опроса контроллеров домена.

6. Нажмите на кнопку **Сохранить**, чтобы применить изменения.
7. Если требуется запустить опрос сети немедленно, нажмите на кнопку **Начать опрос**.

Опрос контроллеров домена с помощью точки распространения

Также можно опрашивать контроллеры домена с помощью точки распространения. Управляемое устройство с операционной системой Windows или Linux может выступать в роли точки распространения.

Для точки распространения с операционной системой Linux поддерживается опрос контроллеров домена Microsoft Active Directory и контроллеров домена Samba.
Для точки распространения с операционной системой Windows поддерживается только опрос контроллеров домена Microsoft Active Directory.
Опрос с помощью точки распространения с операционной системой Mac не поддерживается.

► *Чтобы настроить опрос контроллеров домена с помощью точки распространения:*

1. Откройте свойства точки распространения (см. стр. 258).
2. Выберите раздел **Опрос контроллеров домена**.
3. Выберите параметр **Включить опрос контроллеров домена**.
4. Выберите контроллеры домена, которые вы хотите опросить.

   Если вы используете точку распространения с операционной системой Linux, в разделе **Опрос указанных доменов** нажмите на кнопку **Добавить**, а затем укажите адрес и учетные данные пользователя контроллеров домена.

   Если вы используете точку распространения с операционной системой Windows, можно выбрать один из следующих вариантов:

   - **Опросить текущий домен.**
   - **Опросить весь лес доменов.**
   - **Опросить указанные домены**
5. Нажмите на кнопку **Настроить расписание опроса**, чтобы указать параметры расписания опроса при необходимости.

   Опрос запускается в соответствие с расписанием. Запуск опроса вручную недоступен.

После завершения опроса в разделе **Контроллеры доменов** отобразится структура домена.

Если вы настроили и включили правила перемещения устройств, новые обнаруженные устройства будут автоматически перемещаться в группу **Управляемые устройства** (см. стр. 244). Если правила перемещения устройств не включены, новые обнаруженные устройства будут автоматически перемещаться в группу **Нераспределенные устройства**.

Обнаруженные учетные записи пользователей могут быть использованы для доменной аутентификации в Kaspersky Security Center Web Console (см. стр. 124).

Настройка контроллеров домена Samba

Kaspersky Security Center поддерживает контроллеры домена Linux, работающие только на Samba 4.

Контроллер домена Samba поддерживает те же расширения схемы, что и контроллер домена Microsoft Active Directory. Вы можете включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory, используя расширение схемы Samba 4. Это необязательное действие.

Рекомендуется включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory. Это обеспечит корректное взаимодействие Kaspersky Security Center и контроллера домена Samba.

► *Чтобы включить полную совместимость контроллера домена Samba с контроллером домена Microsoft Active Directory:*

1. Выполните следующую команду, чтобы использовать расширение схемы RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Включите обновление схемы на контроллере домена Samba. Для этого добавьте следующую строку в файл /etc/samba/smb.conf:

   ```
   dsdb:schema update allowed = true
   ```

   Если обновление схемы завершается с ошибкой, необходимо выполнить полное восстановление контроллера домена, который выполняет роль схемы master.

См. также:

Опрос контроллеров домена 178

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 в свойствах инсталляционного пакета Агента администрирования, который будет установлен на временной виртуальной машине (см. стр. 182).

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.

В этом разделе

Включение динамического режима VDI в свойствах инсталляционного пакета Агента администрирования

► *Чтобы включить динамический режим VDI:*

1. В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

   Откроется окно **Свойства**.
3. В окне **Свойства** выберите раздел **Дополнительно**.
4. В разделе **Дополнительно** выберите параметр **Включить динамический режим для VDI**.

Устройство, на которое устанавливается Агент администрирования, будет являться частью VDI.

Перемещение в группу администрирования устройств, являющихся частью VDI

► *Чтобы переместить устройства, являющиеся частью VDI, в группу администрирования:*

1. Перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. На вкладке **Условия правила** выберите вкладку **Виртуальные машины**.

4. Установите для правила **Является виртуальной машиной** значение **Да** и для **Часть Virtual Desktop Infrastructure** значение **Да.**
5. Нажмите на кнопку **Сохранить**.

kaspersky

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

kaspersky

Руководство по усилению защиты

Программа Kaspersky Security Center 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. 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 программ;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы.

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. 43) и их взаимодействием между собой, а также со схемами трафика данных и использования портов (см. стр. 65).

На основании этой информации нужно сформировать архитектуру, определяющую (см. стр. 194):

- расположение Сервера администрирования и подключение к сети;
- организацию рабочих мест администраторов и способы подключения к Серверу администрирования;
- способ установки Агента администрирования и программы защиты;
- 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 файловый сервер соответствует аппаратным и программным требованиям (см. стр. 18).

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.

Учетные записи для установки и запуска Сервера администрирования

Во время развертывания Сервера администрирования необходимо создать две непривилегированные учетные записи (см. стр. 85). Службы, входящие в состав Сервера администрирования, будут работать под этими непривилегированными учетными записями. При предоставлении прав и разрешений учетным записям соблюдайте принцип наименьших привилегий. Избегайте включения ненужных учетных записей в группу kladmins.

Также необходимо создать внутреннюю учетную запись СУБД. Сервер администрирования использует эту внутреннюю учетную запись СУБД для доступа к выбранной СУБД.

Набор необходимых учетных записей и их прав зависит от выбранного типа СУБД и способа создания базы данных Сервера администрирования (см. стр. 109).

kaspersky

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 закрыта (см. стр. 45). Оставшийся порт используется Веб-сервером Kaspersky Security Center (8060) (см. стр. 54). 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 (TLS), используемые Сервером администрирования (см. стр. 171). 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.

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 Web Console. Настроить Сервер администрирования можно таким образом, чтобы пользователи могли подключаться к нему только с устройств с разрешенными IP-адресами (см. стр. 153).

Учетные записи и авторизация

Использование двухэтапной проверки Сервера администрирования

Kaspersky Security Center предоставляет пользователям Kaspersky Security Center Web Console возможность использовать двухэтапную проверку (см. стр. 453) 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 Web Console вы вводите свое имя пользователя, пароль и 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

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

Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Сервера администрирования должен соответствовать следующим требованиям (см. стр. 448):

- 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. 463).

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. 243). Предоставьте этой группе особые права доступа и создайте политику безопасности для нее (см. стр. 444).

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

Ограничение назначения роли Главного администратора

Пользователь, созданный с помощью утилиты kladduser, получает роль Главного администратора в списке контроля доступа (ACL) Сервера администрирования. Рекомендуется избегать назначения роли Главного администратора большому количеству пользователей.

Настройка прав доступа к функциям программы

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Сервера администрирования (см. стр. 432).

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. 552).

  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 программ

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

Рекомендуется использовать отдельную учетную запись для удаленной установки программ. Вы можете назначить роль (см. стр. 450) или разрешения отдельной учетной записи (см. стр. 445).

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 защиты Сервера администрирования

Выбор программы 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 программы 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 защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

Создание отдельной политики безопасности для защиты программы

Для программы 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 Kaspersky Security Center Web Console.

По умолчанию Сервер администрирования использует порт 13299 для приема подключения от Kaspersky Security Center Web Console (см. стр. 45). Рекомендуется ограничить число устройств, с которых Сервер администрирования может управляться по этому порту.

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 вы добавите лицензионный ключ в инсталляционный пакет, лицензионный ключ будет доступен всем пользователям с правами чтения в этой папке (напрямую или через Веб-сервер, встроенный в Сервер администрирования) (см. стр. 54).

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

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства, выполнять развертывание с помощью задачи Добавление лицензионного ключа для управляемой программы, и добавлять код активации или файл ключа на устройства вручную (см. стр. 339).

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования (см. стр. 244).

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.

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. 258).

При необходимости вы также можете просмотреть Отчет о работе точек распространения (см. стр. 432).

Настройка защиты управляемых программ

Политики управляемых программ

Рекомендуется создать политику для каждого вида используемой программы и компонента Kaspersky Security Center (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Agent и другие) (см. стр. 58). Эта групповая 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 программы

Настоятельно рекомендуется включить защиту паролем, чтобы злоумышленники не смогли выключить или удалить программы безопасности "Лаборатории Касперского". На платформах, где поддерживается защита паролем, вы можете установить пароль, например, для Kaspersky Endpoint Security, Агента администрирования и других программ "Лаборатории Касперского" (см. стр. **Error! Bookmark not defined.**). После включения защиты паролем рекомендуется заблокировать соответствующие параметры, закрыв их "замком".

Использование Kaspersky Security Network

Во всех политиках управляемых программ и в свойствах Сервера администрирования рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN (см. стр. 399). 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, периодически запускающую полную проверку устройств.

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с контроллерами доменов и указать диапазоны IP-адресов для обнаружения новых устройств (174).

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

Обслуживание Сервера администрирования

Резервное копирование данных Сервера администрирования

Резервное копирование данных позволяет восстановить данные Сервера администрирования без их потери (см. стр. **Error! Bookmark not defined.**). 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 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 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 проблемы безопасности вы можете настроить функции мониторинга и параметры отчетов (см. стр. 495).

Экспорт событий в SIEM-системы

Для максимально быстрого выявления проблем безопасности до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему (см. стр. 561).

Уведомление по электронной почте о событиях аудита

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений (см. стр. 552) о публикуемых им событиях аудита (см. стр. 531), критических событиях (см. стр. 515), событиях отказа функционирования (см. стр. 519) и предупреждениях (см. стр. 523).

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

kaspersky

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:

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 Web Console.

  Чтобы выполнить развертывание с помощью Консоли администрирования, откройте порт 13291, который используется для приема подключений от Консолей администрирования и закрыт по умолчанию на устройствах с операционными системами, отличными от Windows. Дополнительную информацию см. в следующих разделах: Использование утилиты klscflag для открытия порта 13291 (см. стр. 425).

  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 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 не поддерживает развертывание с использованием групповых политик Microsoft Active Directory®.

О планировании развертывания Kaspersky Security Center в сети организации

Один Сервер администрирования может обслуживать не более чем 20 000 устройств (с MariaDB в качестве СУБД). Если общее количество устройств в сети организации превышает 20 000, следует разместить в сети организации несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

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. 204)). 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. раздел "Типовая конфигурация: множество небольших изолированных офисов" (см. стр. 198).

В разделе "Типовые конфигурации Kaspersky Security Center" приведены подробные описания типовых конфигураций Kaspersky Security Center (см. стр. 197). При планировании развертывания следует, в зависимости от структуры организации, выбрать наиболее подходящую типовую конфигурацию.

На этапе планирования развертывания следует рассмотреть необходимость задания Серверу администрирования специального сертификата X.509. Задание сертификата X.509 для Сервера администрирования может быть целесообразно в следующих случаях (неполный список):

- для инспекции SSL трафика посредством SSL termination proxy или для использования Reverse Proxy;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Выбор структуры защиты организации

Выбор структуры защиты организации определяют следующие факторы:

- Топология сети организации.
- Организационная структура.
- Число сотрудников, отвечающих за защиту сети, и распределение обязанностей между ними.
- Аппаратные ресурсы, которые могут быть выделены для установки компонентов управления защитой.
- Пропускная способность каналов связи, которые могут быть выделены для работы компонентов защиты в сети организации.
- Допустимое время выполнения важных административных операций в сети организации. К важным административным операциям относятся, например, распространение обновлений антивирусных баз и изменение политик для клиентских устройств.

При выборе структуры защиты рекомендуется сначала определить имеющиеся сетевые и аппаратные ресурсы, которые могут использоваться для работы централизованной системы защиты.

Для анализа сетевой и аппаратной инфраструктуры рекомендуется следующий порядок действий:

1. Определить следующие параметры сети, в которой будет развертываться защита:
   - число сегментов сети;
   - скорость каналов связи между отдельными сегментами сети;
   - число управляемых устройств в каждом из сегментов сети;
   - пропускную способность каждого канала связи, которая может быть выделена для функционирования защиты.
2. Определить допустимое время выполнения ключевых операций администрирования для всех управляемых устройств.
3. Проанализировать информацию из пунктов 1 и 2, а также данные нагрузочного тестирования системы администрирования. 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....254

Типовая конфигурация: несколько крупных офисов с собственными администраторами....198

Типовая конфигурация: множество небольших удаленных офисов....198

Начало работы....78

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:

Начало работы....78

В этом разделе

Типовая конфигурация: один офис....198

Типовая конфигурация: несколько крупных офисов с собственными администраторами....198

Типовая конфигурация: множество небольших удаленных офисов....198

kaspersky

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 не более чем 20 000 устройств (с MariaDB в качестве СУБД). 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:

О точках распространения 202

Порты, используемые Kaspersky Security Center 45

Начало работы 78

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. 198). 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. Обратите внимание, что профили подключения Агента администрирования поддерживают только устройства с операционными системами Windows и macOS.

См. также:

Типовая конфигурация: один офис 198

Порты, используемые Kaspersky Security Center 45

Типовая конфигурация: множество небольших удаленных 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*, 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 вы можете 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 разделе: Включение push-сервера (см. стр. 263).

См. также:

О точках распространения 202

Предоставление доступа к Серверу администрирования из интернета 200

Порты, используемые Kaspersky Security Center 45

Выбор СУБД

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

Таблица 15. Рекомендации и ограничения СУБД

СУБД	Рекомендации и ограничения
MySQL (см. поддерживаемые версии на стр. 18)	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 20 000 устройств.
MariaDB (см. поддерживаемые версии на стр. 18)	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 20 000 устройств.
PostgreSQL, Postgres Pro (см. поддерживаемые версии на стр. 18)	Используйте эту СУБД, если вы планируете использовать один Сервер администрирования менее чем для 50 000 устройств.

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

Рекомендуется отключить задачу инвентаризации программного обеспечения и отключить (в параметрах политики Kaspersky Endpoint Security) уведомления Сервера администрирования о запуске программ.

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. 82), PostgreSQL (см. стр. 83) или Postgres Pro (см. стр. 83) используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

См. также:

Учетные записи для работы с СУБД 109

Начало работы 78

Предоставление доступа к Серверу администрирования из интернета

В ряде случаев необходимо предоставить доступ к Серверу администрирования из интернета:

- Регулярное обновление баз, программных модулей и программ "Лаборатории Касперского".
- Обновление программ сторонних производителей

  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. Сервер администрирования должен быть подключен к интернету в следующих случаях:

  - Когда вы используете Сервер администрирования в роли WSUS-сервера.
  - Для установки обновлений программ сторонних производителей, отличных от программ Microsoft.
- Закрытие уязвимостей в программах сторонних производителей

  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.
- Для управления устройствами (ноутбуками) автономных пользователей.
- Для управления устройствами, находящимися в удаленных офисах.
- При взаимодействии с главным или подчиненными Серверами администрирования, находящимися в удаленных офисах.
- для управления мобильными устройствами.

В этом разделе рассмотрены типичные способы обеспечения доступа к Серверу администрирования из интернета. Во всех случаях предоставления доступа к Серверу администрирования из интернета может понадобиться задать Серверу администрирования специальный сертификат.

kaspersky

См. также:

В этом разделе

Сервер администрирования в локальной сети

Если Сервер администрирования располагается во внутренней сети организации, вы можете сделать порт Сервера администрирования 13000 TCP доступным извне с помощью механизма "Port Forwarding". Если требуется управление мобильными устройствами, вы можете сделать TCP-порт 13292 доступным.

См. также:

Доступ из интернета: Сервер администрирования в демилитаризованной зоне

Если Сервер администрирования располагается в демилитаризованной зоне сети организации, у него отсутствует доступ во внутреннюю сеть организации. Как следствие, возникают следующие ограничения:

- Сервер администрирования не может самостоятельно обнаруживать новые устройства.
- Сервер администрирования не может выполнять первоначальное развертывание Агента администрирования посредством принудительной установки на устройства внутренней сети организации.
- Речь идет только о первоначальной установке Агента администрирования. Последующие обновления версии Агента администрирования или установка программы безопасности уже могут быть выполнены Сервером администрирования.

Обратите внимание, что Kaspersky Security Center не поддерживает развертывание с использованием групповых политик Microsoft Windows.

Вы можете использовать точки распространения, расположенные в сети организации. Для выполнения первоначального развертывания на устройствах без Агента администрирования следует предварительно установить Агент администрирования на одно из устройств и назначить это устройство точкой распространения. В результате первоначальная установка Агента администрирования на прочие устройства будет выполняться Сервером администрирования через эту точку распространения.

Для успешной отправки уведомлений управляемым устройствам, размещенным во внутренней сети организации, на порт 15000 UDP, следует покрыть всю сеть предприятия точками распространения. В свойствах назначенных точек распространения установите флажок **Не разрывать соединение с Сервером**

администрирования. В результате Сервер администрирования будет иметь постоянную связь с точками распространения, а точки распространения смогут посылать уведомления на порт 15000 UDP устройствам, размещенным во внутренней сети организации (это может быть IPv4-сеть или IPv6-сеть) (см. стр. 202).

См. также:

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.....75

Доступ из интернета: Использовать 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 с обратным направлением подключения (Сервер администрирования устанавливает соединение с Агентом администрирования) (см. стр. 64). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить Агент администрирования (см. стр. 229). При установке Агента администрирования в окне **Шлюз соединения** мастера установки выберите **Использовать в качестве шлюза соединения в демилитаризованной зоне**.
- Устройство с установленным шлюзом соединения необходимо добавить в качестве точки распространения. Когда вы добавляете шлюз соединения, в окне **Добавить точку распространения** выберите параметр **Выбрать → Добавить шлюз соединений, находящийся в демилитаризованной зоне, по адресу**.
- Чтобы использовать интернет для подключения внешних настольных компьютеров к Серверу администрирования, необходимо изменить инсталляционный пакет Агента администрирования. В свойствах созданного инсталляционного пакета выберите параметр **Дополнительно → Подключаться к Серверу администрирования через шлюз соединения** и укажите вновь созданный шлюз соединения.

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.

О точках распространения

Устройства с установленным Агентом администрирования могут быть использованы в качестве точки распространения. В этом режиме Агент администрирования может распространять обновления, которые могут быть получены как с Сервера администрирования, так и с серверов "Лаборатории Касперского". В последнем случае настройте загрузку обновлений для точки распространения (см. стр. 491).

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. 263).

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 253

Начало работы 78

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 16. 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/10,000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Таблица 17. 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/10,000 + 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 18. 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 19. 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".....468

Типовая конфигурация: множество небольших удаленных офисов.....198

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. В дополнение к структуре групп администрирования, предназначенной для назначения устройствам политик и задач, каждый виртуальный Сервер администрирования имеет собственную группу нераспределенных устройств, собственные наборы отчетов, выборки устройств и события, инсталляционные пакеты, правила перемещения и т. д. Функциональность виртуальных Серверов администрирования может быть использована как поставщиками услуг (xSP) 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.

kaspersky

Сетевые параметры для взаимодействия с внешними сервисами

Kaspersky Security Center использует следующие сетевые параметры для взаимодействия с внешними сервисами.

Таблица 20. Сетевые параметры

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com/activation-service/activationservice.svc	Активация программы.
Порт: 443 Протокол: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Обновление баз и программ "Лаборатории Касперского" (см. стр. 471).
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	• Обновление баз и программ "Лаборатории Касперского" (см. стр. 471). • Проверка если серверы "Лаборатории Касперского" доступны. 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. 171).

Сетевые параметры	Адрес	Описание
Порт: 80 Протокол: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Обновление баз и программ "Лаборатории Касперского" (см. стр. 471).
Порт: 443 Протокол: HTTPS	ds.kaspersky.com	Использование Kaspersky Security Network (см. стр. 399).

Сетевые параметры	Адрес	Описание
Порт: 443, 1443 Протокол: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Использование Kaspersky Security Network (см. стр. 399).
Протокол: HTTPS	click.kaspersky.com redirect.kaspersky.com	Переход по ссылкам из интерфейса.
Порт: 80 Протокол: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Инфраструктура открытых ключей (Public Key Infrastructure, PKI).
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления (см. стр. 559).

Для корректного взаимодействия Kaspersky Security Center с внешними службами соблюдайте следующие рекомендации:
- Незашифрованный сетевой трафик должен быть разрешен на портах 443 и 1443 на сетевом оборудовании и прокси-сервере вашей организации.
- При взаимодействии Сервера администрирования с серверами обновлений "Лаборатории Касперского" и серверами Kaspersky Security Network необходимо избегать перехвата сетевого трафика с подменой сертификатов (MITM-атаки).

Если вы хотите загружать обновления по протоколу HTTP, выполните одну из следующих команд (см. стр. 471):

- На устройство с Сервером администрирования:

  ```
  klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
  ```

- На точку распространения:

  ```
  klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
  ```

Если вы хотите загружать обновления по протоколу HTTPS, выполните одну из следующих команд (см. стр. 471):

- На устройство с Сервером администрирования:

  ```
  klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
  ```

- На точку распространения:

  ```
  klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
  ```

kaspersky

Развертывание Агента администрирования и программы безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенной программы 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 установка 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. 197);
- 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).

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 тихой установки программ на группы устройств. В типичном случае администратор должен централизованно указать значения параметров, которые в дальнейшем могут быть использованы для тихой установки на выбранные устройства в сети.

Инсталляционные пакеты;

Первый и основной способ настройки инсталляционных параметров программ является универсальным и подходит для всех способов установки программ: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов программ.

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 программ.

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 поддерживаемой программ, можно задавать в пользовательском интерфейсе Консоли администрирования при создании инсталляционного пакета. В случае удаленной установки программ средствами Kaspersky Security Center инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора программы ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки программ "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. 124).

Не указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей.

Развертывание с помощью механизма групповых политик Microsoft Windows не поддерживается.

Сразу после установки Kaspersky Security Center автоматически создается несколько инсталляционных пакетов, готовых к установке, в том числе пакеты Агента администрирования и программы безопасности для платформы Microsoft Windows.

Несмотря на то, что лицензионный ключ для лицензии на программу можно задать в свойствах инсталляционного пакета, желательно не использовать этот способ распространения лицензий из-за широкой доступности инсталляционных пакетов на чтение. Следует использовать автоматически распространяемые лицензионные ключи или задачи установки лицензионных ключей.

О задачах удаленной установки программ Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки программ, реализованные в виде задач удаленной установки программ (принудительная установка, установка с помощью копирования образа жесткого диска). 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 другой программы), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки программ, в основе которого также лежит создание задачи удаленной установки программ 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 дисков используйте сторонние инструменты, доступные в организации.

Копирование образа жесткого диска сторонними инструментами

При использовании сторонних инструментов для захвата образа устройства с установленным Агентом администрирования следует воспользоваться одним из следующих методов:

- 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.
- Использовать режим клонирования диска Агента администрирования (см. стр. 213).

Если образ жесткого диска был скопирован неправильно, вы можете решить эту проблему.

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. также:

Режим клонирования диска Агента администрирования.....213

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.
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 212

Принудительное развертывание с помощью задачи удаленной установки программ 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. Только назначенные точки распространения могут выполнять принудительное развертывание на устройствах под управлением Windows из административного ресурса. 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).
- На устройствах должны быть открыты следующие порты для удаленного доступа к устройствам средствами Windows: TCP 139, TCP 445, UDP 137, 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 программ – 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 программ 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 другой программы (например, программы безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другой программы, 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 программ, 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.

Удаленная установка программ 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 программы.

Эта функция включается параметром **Использовать Агент администрирования** в свойствах задачи удаленной установки программ (см. стр. 212).

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. 253). 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 программ (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:

- **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 программы (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах.

Мониторинг развертывания

Чтобы контролировать развертывание Kaspersky Security Center и убедиться, что программа безопасности и Агент администрирования установлены на управляемых устройствах, используйте функции мониторинга и отчеты (см. стр. 496):

- Используйте веб-виджет развертывания в панели инструментов для мониторинга развертывания в режиме реального времени (см. стр. 499).
- Используйте отчеты, чтобы получить подробную информацию (см. стр. 505).

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.

kaspersky

В этом разделе

Общая информация

Установщики компонентов Kaspersky Security Center для устройств под управлением Windows построены по 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 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
```

   Запустится программа установки Kaspersky Security Center.

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:

Общая информация 219
Частичная настройка параметров установки через setup.exe 220
Параметры установки Сервера администрирования 221
Параметры установки Агента администрирования 223
Начало работы 78

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:

Общая информация 219
Установка в тихом режиме (с файлом ответов) 219
Параметры установки Сервера администрирования 221
Параметры установки Агента администрирования 223

Параметры установки Сервера администрирования

В таблице ниже описаны свойства, которые вы можете настроить при установке Kaspersky Security Center в тихом режиме.

Таблица 21. Параметры установки Сервера администрирования в тихом режиме

Имя переменной	Обязательная	Описание	Возможные значения
EULA_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Лицензионного соглашения.	1
PP_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Политики конфиденциальности.	1
KLSRV_UNATT_SERVERADDRESS	Да	DNS-имя Сервера администрирования или статический IP-адрес.	DNS-имя устройства или IP-адрес.
KLSRV_UNATT_PORT_SRV	Нет	Номер порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 14000.	Номер порта
KLSRV_UNATT_PORT_SRV_SSL	Нет	Номер SSL-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13000.	Номер порта
KLSRV_UNATT_PORT_KLOAPI	Нет	Номер KLOAPI-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13299.	Номер порта
KLSRV_UNATT_PORT_GUI	Нет	Номер GUI-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13291.	Номер порта
KLSRV_UNATT_NETRANGETYPE	Нет	Примерное количество устройств, которыми вы планируете управлять. Необязательный параметр. По умолчанию указано значение 1.	1 от 1 до 100 сетевых устройств. 2 от 101 до 1000 сетевых устройств. 3 более 1000 сетевых устройств.
KLSRV_UNATT_DBMS_TYPE	Да	Тип системы управления базой данных: MySQL (MariaDB) или Postgres.	mysql или postgres
KLSRV_UNATT_DBMS_INSTANCE	Да	IP-адрес сервера базы данных.	IP-адрес;
KLSRV_UNATT_DBMS_PORT	Да	Порт сервера базы данных. Значение по умолчанию для MySQL (MariaDB) – 3306; для Postgres – 5432.	3306 или 5432
KLSRV_UNATT_DB_NAME	Да	Имя базы данных.	kav
KLSRV_UNATT_DBMS_LOGIN	Да	Имя пользователя, имеющего доступ к базе данных.	
KLSRV_UNATT_DBMS_PASSWORD	Да	Пароль пользователя, который имеет доступ к базе данных.	

KLSRV_UNATT_KLADMINSGROUP	Да	Имя группы безопасности для служб.	kladmins
KLSRV_UNATT_KLSRVUSER	Да	Имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Да	Имя учетной записи для запуска других служб. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc

Если Сервер администрирования будет развернут как Отказоустойчивый кластер "Лаборатории Касперского" (см. стр. 99), файл ответов должен включать следующие дополнительные переменные:

KLFOC_UNATT_NODE	Да	Номер узла (1 или 2).	1 или 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Да	Точка подключения общей папки состояния.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Да	Точка подключения общей папки данных.	
KLFOC_UNATT_CONN_MODE	Да	Режим подключения отказоустойчивого кластера.	VirtualAdapter Или ExternalLoadBalancer

Если переменная C_UNATT_CONN_MODE имеет значение VirtualAdapter, файл ответов должен включать следующие дополнительные переменные:

KLFOC_UNATT_CONN_MODE_VA_NAME		Имя виртуального сетевого адаптера.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Требуется одна из этих переменных	IP-адрес виртуального сетевого адаптера.	IP-адрес;
KLFOC_UNATT_CONN_MODE_VA_IPV6		IPv6-адрес виртуального сетевого адаптера.	IPv6-адрес.

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 22. Параметры установки Агента администрирования в тихом 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. 330). • 0 – Я не принимаю условия Лицензионного соглашения (установка не выполняется). • 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. • 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.
SERVERSSLPORT	Номер порта для защищенного подключения к Серверу администрирования с использованием протокола SSL.	Числовое значение.
USESSL	Использовать ли SSL-соединение.	• 1 – использовать; • другое значение или не задано – не использовать.
OPENUDPPORT	Открыть ли UDP-порт.	• 1 – открывать; • другое значение или не задано – не открывать.
UDPPORT	Номер UDP-порта	Числовое значение.
USEPROXY	Использовать ли прокси-сервер.	• 1 – использовать; • другое значение или не задано – не использовать.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Адрес прокси-сервера и номер порта для подключения к прокси-серверу.	Строковое значение.

Свойство MSI	Описание	Доступные значения
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; • 1 – использовать данный Агент администрирования в качестве шлюза соединений; • 2 – подключаться к Серверу администрирования через шлюз соединений.
GATEWAYADDRESS	Адрес шлюза соединений.	Строковое значение.
CERTSELECTION	Способ получения сертификата.	• GetOnFirstConnection – получить сертификат от Сервера администрирования; • 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; • 0 – не включать; • Значение не задано – не включать.
LAUNCHPROGRAM	Запускать ли службу Агента администрирования после установки.	• 1 – запускать; • 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. 227).

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 (в разделе **Дополнительно**) выбрать 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:

Начало работы 78

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 выбрать параметр **Включить динамический режим для VDI**:

- в случае удаленной установки – в окне свойств инсталляционного пакета Агента администрирования (раздел **Дополнительно**) (см. стр. 234);
- в случае интерактивной установки – в мастере установки Агента администрирования.

Параметр **Включить динамический режим для VDI** не следует выбирать 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** выбрать параметр **Хранить события после удаления устройств** и указать максимальное время хранения событий в днях.

См. также:

Начало работы 78

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 Агента администрирования копированием образа диска (см. стр. 212).

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 выбран 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:

Начало работы 78

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.

kaspersky

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".

В этом разделе

См. также:

Начало работы 78

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 15** 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 соединения** мастера установки выберите вариант **Использовать в качестве шлюза соединения 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** выберите 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:

      - Реестр 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 226

Просмотр Политики конфиденциальности 333

Установка Агента администрирования в тихом режиме

Агент администрирования может быть установлен в тихом режиме, то есть без интерактивного ввода параметров установки. Для тихой 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 тихом режиме:*

1. Прочитайте Лицензионное соглашение (см. стр. 330). 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 или %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 тихом режиме, приведены в разделе Параметры установки Агента администрирования (см. стр. 223).

См. также:

Локальная установка плагина управления программой

► *Чтобы установить плагин управления программой,*

на устройстве, где установлена Консоль администрирования, запустите исполняемый файл klcfginst.exe, входящий в дистрибутив 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 тихом режиме

► *Чтобы установить программу в тихом 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. 330) и Политики конфиденциальности соответственно (см. стр. 333). 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 инсталляционный пакет**.
   - Перейдите по ссылке **Создать автономный инсталляционный пакет** в рабочей области инсталляционного пакета.

   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.

kaspersky

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 назначения** 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.

- **Состояние**

  Статус пароля: **Пароль задан** или **Пароль не задан**.

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 требуемых 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 ActiveSync 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:

- **Сервер администрирования**

  Адрес устройства, на котором установлен Сервер администрирования.

- **Порт**

  Номер порта, по которому будет выполняться подключение.

- **SSL-порт**

  Номер порта, по которому будет выполняться подключение с использованием протокола SSL.

- **Use Server certificate**

  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-соединение**

  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.

  UDP-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 Сервера администрирования к Агенту администрирования по протоколу UDP.

  По умолчанию номер UDP-порта – 15000.

- **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**

  Если параметр включен, UDP-порты, используемые Агентом администрирования, будут добавлены в список исключений брандмауэра Microsoft Windows.

  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, во время передачи данных (см. стр. 64).
- 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:
  - **Enable dynamic mode for 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. 573). 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 23. Параметры инсталляционного пакета Агента администрирования

Раздел свойств	Windows	Mac	Linux
Общие	✓	✓	✓
Параметры	✓	—	—
Подключение	✓	✓ (кроме параметров **Открывать порты Агента администрирования в брандмауэре Microsoft Windows** и **Использовать только автоматическое определение прокси-сервера**)	✓ (кроме 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	✓	✓	✓

kaspersky

Управление клиентскими устройствами

В этом разделе описано, как управлять устройствами в группах администрирования.

В этом разделе

См. также:

Сценарий: Настройка защиты сети 349

Параметры управляемого устройства

► *Чтобы просмотреть параметры управляемого устройства:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием нужного устройства.

Откроется окно свойств выбранного устройства.

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.

- **Группа**

  Группа администрирования, в состав которой входит клиентское устройство.

- **Последнее обновление**

  Дата последнего обновления антивирусных баз или программ на устройстве.

- **Видим 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, 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.

Сеть

В разделе **Сеть** отображается следующая информация о сетевых свойствах клиентского устройства:

- **IP-адрес;**

  IP-адрес устройства.

- **Windows-домен**

  Рабочая группа, содержащая устройство.

- **DNS-имя;**

  Имя DNS-домена клиентского устройства.

- **NetBIOS-имя.**

  NetBIOS-имя клиентского устройства.

Операционная система

В разделе **Операционная система** представлена информация об операционной системе, установленной на клиентском устройстве.

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.

- **Постоянная защита**

  Статус текущего состояния постоянной защиты 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.

- **Общее количество обнаруженных 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/12.0/ru-RU/65058.htm.

  Файлы могут быть зашифрованы только на управляемых устройствах, на которых установлен Kaspersky Endpoint Security для Windows.

Статус устройства определен программой

В разделе **Статус устройства, определенный программой** отображается информация о статусе устройства, который определен управляемой программой, установленной на клиентском устройстве. Это состояние устройства может отличаться от того, которое определено Kaspersky Security Center.

Программы

В разделе **Программы** отображается список программ "Лаборатории Касперского", установленных на клиентском устройстве. Вы можете нажать на имя программы, чтобы просмотреть общую информацию о программе, список событий, произошедших на устройстве, и параметры программы.

Активные политики и профили политик

В разделе **Активные политики и профили политик** отображаются списки политик и профилей политик, которые активны на управляемом устройстве.

Задачи

На вкладке **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.

Проблемы безопасности

На вкладке **Проблемы безопасности** можно просматривать, редактировать и создавать проблемы безопасности для клиентского устройства. Проблемы безопасности 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 проблему безопасности. Администратор может указать краткое описание случая и рекомендуемых действий (таких как дисциплинарные действия), которые должны быть предприняты против пользователя в тексте проблемы безопасности, и может добавить ссылку на пользователя или пользователей.

Проблема безопасности, для которой выполнены необходимые действия, называется *обработанным*. Наличие необработанных проблем безопасности может быть выбрано условием для изменения статуса устройства на *Критический* или *Предупреждение*.

В разделе содержится список проблем безопасности, созданных для устройства. Проблемы безопасности классифицируются по уровню важности и типу. Тип проблемы безопасности определяется программой "Лаборатории Касперского" (например, Kaspersky Industrial CyberSecurity for Nodes), в которой была создана проблема безопасности. Обработанные проблемы безопасности можно отметить в списке, установив флажок в столбце **Обработана**.

Теги

На вкладке **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.

Исполняемые файлы

В разделе **Исполняемые файлы** отображаются исполняемые файлы, обнаруженные на клиентском устройстве.

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.

Реестр оборудования

В разделе **Реестр оборудования** можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

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).

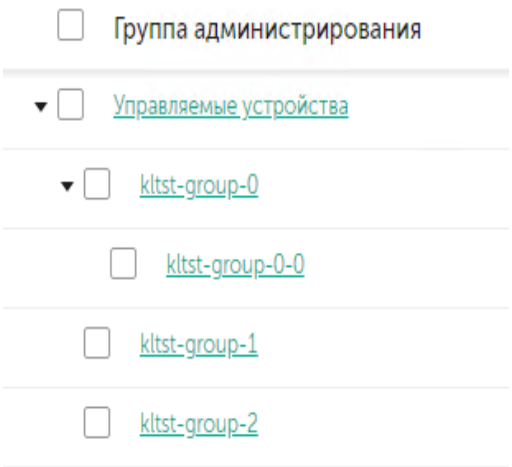


Рисунок 1. Просмотр иерархии групп администрирования

► *Чтобы создать группу администрирования:*

1. В главном окне программы перейдите в раздел **Активы (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.

► *Чтобы создать структуру групп администрирования:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Иерархия групп**.
2. Нажмите на кнопку **Импорт**.

В результате запускается мастер создания структуры групп администрирования. Следуйте далее указаниям мастера.

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 (логического выражения над атрибутами устройства) и целевой группы администрирования (см. стр. 248). 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 разделе **Активы (Устройства)** → **Правила перемещения**.

Правило перемещения по умолчанию предназначено для однократного первоначального размещения устройств в группах администрирования. Правило перемещает нераспределенные устройства только один раз устройства. Если устройство однажды было перемещено этим правилом, правило не переместит его повторно, даже если вернуть устройство вручную в группу нераспределенных устройств. 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, не размещенные в группах администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.
Флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования** заблокирован в свойствах автоматически созданных правил перемещения. Такие правила создаются при добавлении задачи *Удаленная установка программы* или создании автономного инсталляционного пакета.

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, задачи для выборок устройств (см. стр. 59), назначать Агенты администрирования согласно методике (см. стр. 253) и так далее.

См. также:

Начало работы 78

Создание правил перемещения устройств

Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования (см. стр. 244).

Чтобы создать правило перемещения устройств:

1. В главном окне программы перейдите в раздел **Активы (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.
   - **Активное 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.

- **Перемещать только устройства, не принадлежащие группам 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.

- **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).

4. На закладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования (см. стр. 248).
5. Нажмите на кнопку **Сохранить**.

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 250

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 **Активы (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.
   - **Активное 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.
   - **Перемещать только устройства, не принадлежащие группам 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.
   - 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).

5. На вкладке **Условия правила** укажите критерии для устройств, которые требуется переместить автоматически (см. стр. 248).
6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

При создании (см. стр. 245) или копировании (см. стр. 246) правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств (см. стр. 244). 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.

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.

Вкладка Теги

На этой вкладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств (см. стр. 285). 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**

Вкладка Сеть

На этой вкладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **DNS-имя устройства**
- **DNS-домен**
- **Диапазон IP-адресов**
- **IP-адрес подключения к Серверу**
- **Изменение профиля подключения**
- **Под управлением другого Сервера администрирования**

Вкладка Программы

На этой вкладке можно настроить правило перемещения устройств на основе управляемых программ и операционных систем, установленных на клиентских устройствах:

- **Агент администрирования установлен**
- **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**
- **Идентификатор выпуска операционной системы**

Вкладка Виртуальные машины

На этой вкладке можно настроить параметры правила перемещения клиентских 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**

Вкладка Контроллеры домена

На этой вкладке вы можете указать, что требуется перемещать устройства, входящие в организационное подразделение домена. Вы также можете перемещать устройства из всех дочерних подразделений указанного подразделения домена:

- **Устройство входит в следующее подразделение**
- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы контроллера домена.

  По умолчанию параметр выключен.
- **Перемещать устройства из дочерних подразделений в соответствующие подгруппы**
- **Создавать подгруппы, соответствующие контейнерам вновь обнаруженных устройств**
- **Удалять подгруппы, отсутствующие в домене**
- **Устройство включено в следующую группу безопасности домена**

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 **Активы (Устройства)** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь:** `<текущий_путь>` 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 DNS-имя устройства.

       > Поле с именем устройства не должно содержать пробелы, отступы, 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, отступы, 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:

Создание правил перемещения устройств 245

Перемещение устройств или кластеров в состав группы администрирования вручную 251

Перемещение устройств или кластеров в состав группы администрирования вручную

Устройства можно перемещать из одной группы администрирования в другую или из группы нераспределенных устройств в группу администрирования.

Также можно перемещать кластеры или массивы серверов из одной группы администрирования в другую (см. стр. 252). При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования. При выборе одного узла кластера на вкладке **Устройства**, кнопка **Переместить в группу** становится недоступной.

► *Чтобы переместить одно или несколько устройств или кластеров 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 **Активы (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. Если группа администрирования содержит кластеры или массивы серверов, раздел **Управляемые устройства** разделен на две вкладки – **Устройства** и **Кластеры и массивы серверов**. Откройте вкладку объекта, который хотите переместить.
3. Установите флажки рядом с устройствами или кластерами, которые требуется переместить в другую группу.
4. Нажмите на кнопку **Переместить в группу**.
5. В иерархии групп администрирования установите флажок рядом с группой администрирования, в которую вы хотите переместить выбранные устройства или кластеры.
6. Нажмите на кнопку **Переместить**.

Выбранные устройства или кластеры перемещаются в выбранную группу администрирования.

kaspersky

О кластерах и массивах 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.

Если группа администрирования содержит кластеры или массивы серверов, на странице **Управляемые устройства** отображаются две вкладки: одна для отдельных устройств, другая для кластеров и массивов серверов. После обнаружения управляемых устройств в качестве узлов кластера, кластер добавляется как отдельный объект на вкладку **Кластеры и массивы серверов**.

Узлы кластера или массивы серверов перечислены на вкладке **Устройства** вместе с другими управляемыми устройствами. Вы можете просматривать свойства узлов как отдельных устройств и выполнять другие операции, но удалить узел кластера или переместить его в другую группу администрирования отдельно от его кластера нельзя (см. стр. 239). Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Просмотр свойств (см. стр. 252)
- Переместить кластер или массив серверов в другую группу администрирования (см. стр. 251).

  При перемещении кластера или массива серверов в другую группу, все его узлы перемещаются вместе с ним, так как кластер и любой из его узлов всегда принадлежат к одной группе администрирования.
- Удалить

  Целесообразно удалять кластер или массив серверов только тогда, когда кластер или массив серверов больше не существует в сети организации. Если кластер по-прежнему виден в вашей сети, а Агент администрирования и программа безопасности "Лаборатории Касперского" по-прежнему установлена на узлах кластера, Kaspersky Security Center автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

См. также:

Свойства кластера или массива серверов.....252

Свойства кластера или массива серверов

► *Чтобы просмотреть параметры кластера или массива серверов:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → **Кластеры и массивы серверов**.

   Отображается список кластеров и массивов серверов.
2. Нажмите на имя нужного кластера или массива серверов.

Откроется окно свойств выбранного кластера или массива серверов.

Общие

Раздел **Общие** отображает общую информацию о кластере или массиве серверов. Информация предоставляется на основании данных, полученных в ходе последней синхронизации узлов кластера с Сервером

администрирования:

- **Имя.**
- **Описание**
- **Windows-домен**
- **NetBIOS-имя.**
- **DNS-имя;**

Задачи

На вкладке **Задачи** вы можете управлять задачами, назначенными для кластеров и массивов серверов: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять параметры задач и просматривать результаты выполнения. Перечисленные задачи относятся к программе безопасности "Лаборатории Касперского", установленной на узлах кластера. Kaspersky Security Center получает список задач и информацию о статусе задач от узлов кластера. В случае отсутствия связи статус не отображается.

Узлы

На этой вкладке отображается список узлов, входящих в кластер или массив серверов. Вы можете нажать на имя узла, чтобы просмотреть окно свойств устройства (см. стр. 239).

Программ "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к программе безопасности "Лаборатории Касперского", установленной на узлах кластера.

См. также:

О кластерах и массивах серверов 252

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*.

- 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.

kaspersky

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:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского" 468

Начало работы 78

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".....468

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).

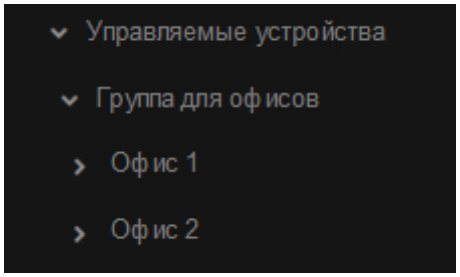


Рисунок 2. Удаленные офисы отражены в структуре групп администрирования

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).

Ноутбук, находившийся в группе администрирования **Офис 1**, но физически перемещенный 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.

kaspersky

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 24. 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/10,000 + 1), рекомендуется: (N/5000 + 2), где N количество устройств в сети

Таблица 25. 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/10,000 + 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 26. 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 27. 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".....468

Типовая конфигурация: множество небольших удаленных офисов.....198

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center будет сам выбирать, 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".....468

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. 204).

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 параметры 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. 204) 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. 204) 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.

- **Run push server**
- Порт push-сервера

- В разделе **Область действия** укажите группы администрирования, которым точка распространения будет распространять обновления.
- 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. 490).

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 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 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/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

- **Игнорировать параметры прокси-сервера для подключения к KPSN**

  Установите этот флажок, если параметры прокси-сервера настроены в свойствах точки распространения или политики Агента администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемой программы не будет передан в KPSN.

  Это параметр доступен, если вы выбрали параметр **Доступ к облачной службе KSN/KPSN 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**

- 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 контроллеров домена с помощью точки распространения.
  - **Опрос контроллеров домена**
- Настройте опрос IP-диапазонов точкой распространения.
  - **Опрос IP-диапазонов.**

    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.

    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.

1. Нажмите на кнопку **ОК**.

В результате выбранные устройства будут выполнять роль точек распространения.

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 **Активы (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 **Активы (Устройства)** → **Точки распространения**.
5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить**.
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.

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. 373) 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 **Запустить push-сервер** 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.

См. также:

Принудительная синхронизация 373

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 28. 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. • Переключатель выключен.
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. • Приостановлена. • Выполняется.

Условие	Описание условия	Доступные значения
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 подключался	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.
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. • Переключатель включен.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.

Условие	Описание условия	Доступные значения
Срок действия лицензии истекает.	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
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). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен программой	Статус устройства определяется управляемой программой.	• Переключатель выключен. • Переключатель включен.
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

Условие	Описание условия	Доступные значения
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Выключена защита	Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени.	Более чем 0 минут.
Не запущена программа безопасности	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Переключатель выключен. • 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 данных 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 данных устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

См. также:

Настройка переключения статусов устройств 551

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 открывшемся окне **Свойства** 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 открывшемся окне **Свойства** 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 29. 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. • Флажок снят.
Найдено много вирусов	В результате работы задач поиска вирусов, например, задачи Поиск вирусов, 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. • Приостановлена. • 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
Обнаружены активные угрозы	Количество необработанных объектов в папке **Необработанные файлы** 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

Условие	Описание условия	Доступные значения
Установлены несовместимые программы	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы.	• Флажок снят. • 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. • Высокий. • Средний. • Игнорировать, если нельзя закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Флажок снят. • 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
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). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.

Условие	Описание условия	Доступные значения
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. • Флажок установлен.
Есть необработанные проблемы безопасности	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. • Флажок установлен.
Статус устройства определен программой	Статус устройства определяется управляемой программой.	• Флажок снят. • Флажок установлен.
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. • Флажок установлен.
Выключена защита	Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени.	Более чем 0 минут
Не запущена программа безопасности	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Флажок снят. • Флажок установлен.

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.

См. также:

Использование выборок событий 535

Сценарий: Настройка защиты сети 349

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 **Активы (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. 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 **Создать задачу**, чтобы создать задачу, которая будет применена к этим устройствам (см. стр. 406).

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 **Активы (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 любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **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. 273), 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 **Активы (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 вкладке **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) или IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Отображаются все устройства, входящие в указанную рабочую группу.

- **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 таких фраз, как **SUSE Linux корпоративный сервер 12** или же **SUSE Linux корпоративный сервер 15**, можно ввести **SUSE Linux Enterprise Server 1?**.

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"**.

- **Диапазон IP-адресов**

  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 **Контроллеры доменов** можно настроить критерии включения устройств в выборку по членству в домене:

- **Устройство в подразделении домена**
- **Это устройство является членом группы безопасности домена**

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:

- **Есть**. 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:

  - **Есть**. 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:

- **Есть**. 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.

Статусы устройств

В разделе **Статус управляемого 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*, *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, Критичный* 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.

- **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.

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 информацию 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.

- **Производитель**

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- **Имя устройства**

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.

- **Производитель 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.

- **Производитель**

  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.

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:

- **Есть**. 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 **Программы "Лаборатории Касперского"** 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.

- **Выбор периода последнего обновления модулей**

  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 Сервера администрирования**

В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center:

- **Есть**. 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.

- **Установлена программа безопасности**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

  - **Есть**. 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 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.

- **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 антивирусной базы.

  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.

- **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.

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).

Доступные значения: *AES56*, *AES128*, *AES192*, и *AES256*.

Подраздел **Компоненты программы** содержит список компонентов тех программ, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center 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:

- **Состояние**
- **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:

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.

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.

пользователей;

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 и экспортировать ее в файл CSV или TXT.

► *Чтобы экспортировать список устройств из выборки устройств:*

1. Откройте таблицу с устройствами из выборки устройств (см. стр. 272).
2. Используйте один из следующих способов для выбора устройств, которые вы хотите экспортировать:
   - Чтобы выбрать определенные устройства, установите флажки рядом с ними.
   - Чтобы выбрать все устройства на текущей странице таблицы, установите флажок в заголовке таблицы устройств, а затем установите флажок **Выбрать все на текущей странице**.
   - Чтобы выбрать все устройства из таблицы, установите флажок в заголовке таблицы устройств, а затем выберите **Выбрать все**.
3. Нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована.

Обратите внимание, если вы отфильтровали таблицу устройств, 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 **Активы (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.

kaspersky

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. 272), при поиске устройств и при распределении устройств по группам администрирования (см. стр. 56).

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, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы CentOS, назначается тег `[CentOS]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства под управлением операционной системы CentOS 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.

Создание тегов устройств

► *Чтобы создать тег устройства:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. В поле **Тег** введите название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов устройства.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Изменение тегов устройств

► *Чтобы переименовать тег устройства:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**.
2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.
3. В поле **Тег** измените название тега.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Удаление тегов устройств

► *Чтобы удалить тег устройства:*

1. В главном окне программы перейдите в раздел **Активы (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. Для того чтобы удалить тег с вашего устройства, используйте утилиту klscflag.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Просмотр устройств, которым назначен тег

► *Чтобы просмотреть устройства с назначенными тегами:*

1. В главном окне программы перейдите в раздел **Активы (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.....174

kaspersky

Просмотр тегов, назначенных устройству

► *Чтобы просмотреть теги, назначенные устройству:*

1. В главном окне программы перейдите в раздел **Активы (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. 288) устройству или удалить назначенный ранее тег (см. стр. 288). Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Назначение тегов устройству вручную

► *Чтобы вручную назначить тег устройству:*

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег (см. стр. 288).
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 существующий 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.....174

Удаление назначенного тега с устройства

► *Чтобы снять назначенный тег с устройства:*

1. В главном окне программы перейдите в раздел **Активы (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. 287).
> Вы не можете вручную удалить теги, назначенные устройству программами или Агентом администрирования. Для того чтобы удалить эти теги, используйте утилиту klscflag.

См. также:

Сценарий: Обнаружение устройств в сети.....174

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 **Активы (Устройства)** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне программы перейдите в раздел **Активы (Устройства)** → **Теги** → **Теги устройств**, а затем перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству (см. стр. 288), и нажмите на кнопку **Свойства**.

Отобразится список правил автоматического назначения тегов устройствам.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Изменение правил автоматического назначения тегов устройствам

► *Чтобы изменить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 289).
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. 290).
   - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры (см. стр. 290).
   - Если вы хотите удалить условие, установите флажок рядом с именем условия, которое требуется удалить, и нажмите на кнопку **Удалить**.
5. В окне с параметрами условий нажмите на кнопку **ОК**.
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Создание правил автоматического назначения тегов устройствам

► *Чтобы создать правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 289).
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, DNS-имя устройства или принадлежность устройства к IP-подсети).

     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.
   - **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. 289).
- После выполнения правила вручную (см. стр. 291).
- 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. 288) в свойствах устройства.

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. 289).
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

См. также:

Сценарий: Обнаружение устройств в сети.....174

Удаление правил автоматического назначения тегов с устройств

► *Чтобы удалить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 289).
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. 287).

См. также:

Сценарий: Обнаружение устройств в сети.....174

Шифрование и защита данных

Шифрование данных снижает риски непреднамеренной утечки информации в случае кражи/утери портативного устройства или жесткого диска. Также шифрование данных предотвращает доступ к данным неавторизованных пользователей и программ.

Вы можете использовать функцию шифрования данных, если в вашей сети есть управляемые устройства с операционной системой Windows, на которых установлена программа Kaspersky Endpoint Security для Windows. В этом случае можно управлять следующими типами шифрования:

- шифрование диска BitLocker на устройствах под управлением операционной системы Windows для серверов;

- шифрование диска Kaspersky на устройствах под управлением операционной системы Windows для рабочих станций.

С помощью этих компонентов Kaspersky Endpoint Security для Windows вы можете, например, включать или выключать шифрование https://support.kaspersky.com/KESWin/12.0/ru-RU/128080.htm, просматривать список зашифрованных жестких дисков (см. стр. 293), формировать и просматривать отчеты о шифровании (см. стр. 295).

Чтобы настроить шифрование, настройте политику Kaspersky Endpoint Security для Windows в Kaspersky Security Center. Kaspersky Endpoint Security для Windows выполняет шифрование и расшифровку в соответствии с активной политикой. Подробные инструкции по настройке правил и описание особенностей шифрования см. в онлайн-справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/128080.htm.

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса (см. стр. 171).

См. также:

В этом разделе

Просмотр списка зашифрованных жестких дисков

В Kaspersky Security Center вы можете просмотреть информацию о зашифрованных жестких дисках и об устройствах, зашифрованных на уровне дисков. После того, как информация на диске будет расшифрована, диск будет автоматически удален из списка.

► *Чтобы просмотреть список зашифрованных жестких дисков,*

В главном окне программы перейдите в раздел **Операции** → **Шифрование и защита данных** → **Зашифрованные жесткие диски**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела (см. стр. 171).

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

См. также:

Сценарий: Настройка защиты сети 349

Просмотр списка событий шифрования

В процессе выполнения задач шифрования или расшифровки данных на устройствах Kaspersky Endpoint Security для Windows отправляет в Kaspersky Security Center информацию о возникающих событиях следующих типов:

- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за нехватки места на диске;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за проблем с лицензией;
- невозможно зашифровать или расшифровать файл или создать зашифрованный архив из-за отсутствия прав доступа;
- программе запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

► *Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:*

В главном окне программы перейдите в раздел **Операции** → **Шифрование и защита данных** → **События шифрования**.

Если раздела нет в меню, значит, он скрыт. В настройках пользовательского интерфейса включите параметр **Показать раздел "Шифрование и защита данных"** для отображения раздела (см. стр. 171).

Вы можете экспортировать список зашифрованных жестких дисков в файлы форматов CSV или TXT. Для этого нажмите на кнопку **Экспортировать в CSV** или **Экспортировать в TXT**.

Также можно просмотреть список событий шифрования для каждого управляемого устройства.

► *Чтобы просмотреть события шифрования управляемого устройства:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя управляемого устройства.
3. На вкладке **Общие** перейдите в раздел **Защита**.
4. Перейдите по ссылке **Просмотреть ошибки шифрования данных**.

См. также:

Сценарий: Настройка защиты сети 349

kaspersky

Формирование и просмотр отчетов о шифровании

Вы можете формировать следующие отчеты:

- Отчет о статусе шифрования управляемых устройств. В этом отчете представлены сведения о шифровании данных различных управляемых устройств. Например, в отчете показано количество устройств, к которым применяется политика с настроенными правилами шифрования. Также можно узнать, например, сколько устройств нужно перезагрузить. Отчет также содержит информацию о технологии и алгоритме шифрования для каждого устройства.
- Отчет о статусе шифрования запоминающих устройств. Этот отчет содержит похожую информацию, что и отчет о состоянии шифрования управляемых устройств, но предоставляет данные только для запоминающих устройств и съемных дисков.
- Отчет о правах доступа к зашифрованным дискам. Этот отчет показывает, какие учетные записи пользователей имеют доступ к зашифрованным жестким дискам.
- Отчет об ошибках шифрования файлов. Отчет содержит информацию об ошибках, которые возникли при выполнении задач шифрования или расшифровки данных на устройствах.
- Отчет о блокировании доступа к зашифрованным файлам. Отчет содержит информацию о блокировке доступа программ к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или программа пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг и отчеты** → **Отчеты** (см. стр. 510). Также в разделе **Операции** → **Шифрование и защита данных**, можно создавать следующие отчеты о шифровании:

- Отчет о статусе шифрования запоминающих устройств.
- Отчет о правах доступа к зашифрованным дискам.
- Отчет об ошибках шифрования файлов.

► *Чтобы сгенерировать отчет шифрования в разделе **Шифрование и защита данных**:*

1. Убедитесь, что параметр **Шифрование и защита данных** в параметрах интерфейса включен (см. стр. 171).
2. В главном окне программы перейдите в раздел **Операции** → **Шифрование и защита данных**.
3. Откройте один из следующих разделов:
   - **Зашифрованные жесткие диски** – формирует отчет о состоянии шифрования запоминающих устройств или отчет о правах доступа к зашифрованным жестким дискам.
   - **События шифрования** – формирует отчет об ошибках шифрования файлов.
4. Выберите название отчета, который требуется сгенерировать.

Запустится процесс формирования отчета.

См. также:

Сценарий: Настройка защиты сети 349

Предоставление доступа к зашифрованному жесткому диску в автономном режиме

Пользователь может запросить доступ к зашифрованному устройству, например, если Kaspersky Endpoint Security для Windows не установлен на управляемом устройстве. После получения запроса вы можете создать файл ключа доступа и отправить его пользователю. Все варианты использования и подробные инструкции приведены в онлайн-справке Kaspersky Endpoint Security для Windows.

► *Чтобы предоставить доступ к зашифрованному жесткому диску в автономном режиме:*

1. Получите файл запроса доступа от пользователя (файл с расширением FDERTC). Следуйте инструкциям в онлайн-справке Kaspersky Endpoint Security для Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/130941.htm.
2. В главном окне программы перейдите в раздел **Операции → Шифрование и защита данных → Зашифрованные жесткие диски**.

   Отобразится список зашифрованных жестких дисков.
3. Выберите диск, у которому пользователь запросил доступ.
4. Нажмите на кнопку **Предоставить доступ к устройству в автономном режиме**.
5. В открывшемся окне выберите плагин Kaspersky Endpoint Security для Windows.
6. Следуйте инструкциям, приведенным в онлайн-справке Kaspersky Endpoint Security для Windows (см. инструкции для Kaspersky Security Center Web Console в конце раздела) https://support.kaspersky.com/KESWin/12.0/ru-RU/130941.htm.

После этого пользователь может использовать полученный файл для доступа к зашифрованному жесткому диску и чтения данных, хранящихся на диске.

См. также:

Список поддерживаемых программ "Лаборатории Касперского".....37

Сценарий: Настройка защиты сети.....349

Смена Сервера администрирования для клиентских устройств

Вы можете сменить Сервер администрирования на другой для конкретных клиентских устройств. Для этого используйте задачу *Сменить Сервер 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 (см. стр. 408).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера создания задачи **Новая задача** выберите программу **Kaspersky Security Center 15** и тип задачи **Сменить**

Сервер администрирования. Затем укажите устройства, для которых вы хотите сменить Сервер администрирования:

- **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 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.

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 *Сменить Сервер 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 справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/help/KESWin/12.0/ru-RU/128089.htm.

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 **Активы (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 в сети** 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.

kaspersky

Развертывание программ "Лаборатории Касперского"

В этом разделе описано, как развернуть программы "Лаборатории Касперского" на управляемых устройствах в вашей организации с помощью Kaspersky Security Center Web Console.

В этом разделе

Сценарий: Развертывание программ "Лаборатории Касперского"

В этом сценарии описана процедура развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console. Можно либо воспользоваться мастером первоначальной настройки (см. стр. 129) и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Следующие программы доступны для развертывания с помощью Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security для Linux;
- Kaspersky Endpoint Security для Windows.

kaspersky

Этапы

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

1. Загрузка веб-плагина управления программы

   Этот этап обрабатывается мастером первоначальной настройки. Если вы решите не запускать мастер, загрузите плагины вручную.

2. Загрузка и создание инсталляционных пакетов

   Этот этап обрабатывается мастером первоначальной настройки.

   Мастер первоначальной настройки позволяет загрузить инсталляционный пакет совместно с веб-плагином управления. Если вы не выбрали этот параметр при запуске мастера или не запускали мастер, требуется загрузить инсталляционный пакет вручную (см. стр. 302).

   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 для программ (см. стр. 305). Если вы используете автономные пакеты для установки программ "Лаборатории Касперского", вам не нужно создавать и запускать задачу удаленной установки, а также создавать и настраивать задачи для Kaspersky Endpoint Security для Windows.

   Также можно загрузить дистрибутивы Агента администрирования и программ безопасности с сайта "Лаборатории Касперского" https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint. Если удаленная установка программ по каким-либо причинам невозможна, вы можете использовать загруженные дистрибутивы для локальной установки программ.

3. 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. 408) 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. 315), чтобы настроить Агент администрирования.

4. Создание и настройка задач

   Задача *Обновление* Kaspersky Endpoint Security 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. 408) и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи (см. стр. 410) соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

5. Создание политик

   Создайте политику Kaspersky Endpoint Security для Linux вручную (см. стр. 367) 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. 367) политики в соответствии с вашими требованиями.

6. Проверка результатов

   Убедитесь, 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.

Добавление плагина управления для программ "Лаборатории Касперского"

Чтобы развернуть программу "Лаборатории Касперского", такую как Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows, необходимо загрузить веб-плагин управления для этой программы.

► *Чтобы загрузить веб-плагин управления для программы "Лаборатории Касперского":*

1. В главном окне программы перейдите в раздел **Параметры** → **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 для Linux).

   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. Загрузите веб-плагины управления с веб-сайта "Лаборатории Касперского" https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.

► *Чтобы загрузить или обновить веб-плагин управления из файла:*

1. В главном окне программы перейдите в раздел **Параметры** → **Веб-плагины**.
2. Укажите файл плагина и подпись файла:
   - 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.

Веб-плагин управления будет загружен из файла и появится в списке веб-плагинов управления.

См. также:

Веб-плагин управления 57
Сценарий: Развертывание программ "Лаборатории Касперского" 299

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. 546). 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 из файла для программ "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 Linux.

   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 и создать инсталляционный пакет** отображается кнопка **Загрузить 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 вкладке **Загружен**. 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:

   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:

Просмотр экранных уведомлений 546

Сценарий: Развертывание программ "Лаборатории Касперского" 299

kaspersky

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любую программу (такую как текстовый редактор) на клиентские устройства, например, с помощью задачи (см. стр. 406);
- создать автономный инсталляционный пакет (см. стр. 305).

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.

► *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**.
5. В открывшемся окне выберите файл архива, 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.

   Начнется загрузка файла на Сервер администрирования.
6. Если вы указали файл программы "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение (см. стр. 330) для этой программы. Чтобы продолжить, вы должны принять условия Лицензионного соглашения. Выберите параметр **Принять положения и условия настоящего Лицензионного соглашения** только в том случае, если вы полностью прочитали, поняли и приняли условия Лицензионного соглашения.

   Также вам будет предложено прочитать и принять условия Политики конфиденциальности (см. стр. 333). Чтобы продолжить, вы должны принять условия Политики конфиденциальности. Выберите параметр **Я принимаю условия Политики конфиденциальности**, только если вы понимаете и соглашаетесь с тем, что ваши данные будут обрабатываться и передаваться (в том числе в третьи страны), как описано в Политике конфиденциальности.
7. 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.

8. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования (см. стр. 124). 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:
  - **Название**. 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.
  - **Создан**. Дата создания инсталляционного пакета.
  - **Изменен**. Дата изменения инсталляционного пакета.
  - **Тип**. Тип инсталляционного пакета.
- Измените параметры командной строки.

См. также:

Просмотр экранных уведомлений 546

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, 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 создать автономный инсталляционный пакет для программ "Лаборатории Касперского", так и для программ сторонних производителей. Чтобы создать автономный инсталляционный пакет для программ сторонних производителей, необходимо создать пользовательский инсталляционный пакет (см. стр. 304).

Убедитесь, что автономный инсталляционный пакет не доступен для третьих 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 выбран параметр **Не перемещать устройства**. Если вы не хотите перемещать клиентское устройство ни в какую группу администрирования после установки Агента администрирования, не изменяйте этот параметр.

   Если вы хотите переместить клиентское устройство после установки Агента администрирования, выберите параметр **Переместить 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. 124). 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" 299

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. 85).
2. Измените текущую папку на папку установки Kaspersky Security Center (обычно это /opt/kaspersky/ksc64/sbin).
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
     ```

   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.

kaspersky

Установка Агента администрирования для Linux в 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 режиме, то есть без участия пользователя.

► *Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:*

1. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 315) и настройте Агент администрирования.
2. Прочитайте Лицензионное соглашение (см. стр. 330). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
3. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. 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 тихом режиме

5. 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 тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Установка Агента администрирования 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 Linux, работает один из поддерживаемых дистрибутивов Linux (см. стр. 18).
- Загрузите 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. 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`.

b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

c. 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 целевое устройство работает под управлением Astra Linux, в файл /etc/sudoers добавьте последней строку со следующим текстом: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. Сохраните и закройте файл sudoers.

e. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

3. 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`.

Добавьте `строку экспорта PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<username>/.bashrc`, где `<username>` — учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
$ sudo systemctl restart systemd-logind.service
```

4. Откройте файл /etc/digsig/digsig_initramfs.conf и укажите следующие параметры:

```
DIGSIG_ELF_MODE=1
```

5. В командной строке введите следующую команду, чтобы установить совместимый пакет:

```
apt install astra-digsig-oldkeys
```

6. Создайте директорию для ключа программы:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Поместите ключ программы в директорию /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg, созданную на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

Если в комплект поставки Kaspersky Security Center не входит ключ kaspersky_astra_pub_key.gpg, вы можете загрузить этот ключ по ссылке https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Обновите оперативную память дисков:

   ```
   update-initramfs -u -k all
   ```

   Перезагрузите систему.

9. 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_<номер сборки>_arm64.deb
     ```

Агент администрирования для Linux.

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 **Просмотр списка автономных инсталляционных 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 почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

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 **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

4. На странице **Новая задача** из раскрывающегося списка **Программа** выберите **Kaspersky Security Center**. Затем в раскрывающемся списке **Тип задачи** выберите **Распространение инсталляционного пакета** и укажите имя задачи.

5. На странице **Область действия** 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 **Указать 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. 410). 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.

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`.

b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

c. 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`

d. Сохраните и закройте файл sudoers.

e. Повторно подключитесь к устройству через SSH и проверьте, что служба sudo не требует пароль, с помощью команды `sudo whoami`.

3. 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`.

Если целевое устройство работает под управлением Astra Linux, добавьте `строку экспорта PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<username>/.bashrc`, где `<username>` — учетная запись пользователя, которая будет использоваться для подключения устройства с помощью SSH.

Чтобы применить измененный параметр, перезапустите устройство под управлением Linux или выполните следующую команду:

```
$ sudo systemctl restart systemd-logind.service
```

4. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 315) и настройте Агент администрирования.

5. 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.

6. 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.
- На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

7. 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.

После подготовки устройства с операционной системой SUSE Linux Enterprise Server 15, установите Агент администрирования (см. стр. 299).

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 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. 326).

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 адресами или на выборку устройств.

► *Чтобы установить программу на выбранные устройства:*

1. В главном окне программы перейдите к закладке **Активы (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 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.

   Задача *Удаленная установка программы* создана для указанных устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.

5. На шаге **Область действия** укажите группу администрирования, устройства с определенными адресами или выборку устройств.

   Доступные параметры зависят от параметра, выбранного на предыдущем шаге.

6. На шаге **Инсталляционные пакеты** укажите следующие параметры:

   - В поле **Выбор инсталляционного пакета** выберите инсталляционный пакет программы, которую требуется установить.
   - 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 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.

Единственный способ установить программу для Windows (включая Агент администрирования для Windows) на устройство, на котором не установлен Агент администрирования, – это использовать точку распространения с операционной системой Windows. Поэтому при установке программы для Windows:

- Выберите этот параметр.
- Убедитесь, что для целевых клиентских устройств назначена точка распространения.
- Убедитесь, что на точке распространения установлена операционная система Windows.

- **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.

- В поле **Максимальное количество одновременных загрузок** укажите максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы.
- В поле **Максимальное количество попыток установок** укажите максимально допустимое количество запусков программы установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky Security Center больше не запускает программу установки на устройстве. Чтобы перезапустить задачу *Удаленная установка программы*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка программы*.

- Настройте дополнительный параметр:

  - **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.

  - **Предварительно проверять тип операционной системы перед загрузкой**
  - **Предлагать пользователю закрыть работающие программы**

    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.

- Выберите, на какие устройства вы хотите установить программу:
  - **Установить на все устройства**

    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 администрирования**

    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 между ними.
- Укажите, следует ли перемещать устройства в группу администрирования после установки:
  - **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 выбранную группу (можно выбрать только одну группу)**

    Устройства перемещаются в выбранную вами группу администрирования.

  Обратите внимание, что по умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

1. На этом шаге мастера укажите, требуется ли перезагрузка устройства при установке программ:
   - **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.
2. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка программы*:
   - **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 (Агент администрирования не используется)**

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. На шаге **Завершение создания задачи** нажмите на кнопку **Готово**, чтобы создать задачу и закрыть мастер.

   Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи. В этом окне можно проверить параметры задачи, изменить их или при необходимости настроить расписание запуска задачи.

2. В списке задач выберите созданную задачу и нажмите на кнопку **Запустить**.

   Или дождитесь запуска задачи в соответствии с расписанием, указанным в параметрах задачи.

После выполнения задачи удаленной установки, выбранная программа устанавливается на указанный набор устройств.

См. также:

Мастер развертывания защиты 136

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. 326). Следуйте далее указаниям мастера.
2. На странице **Параметры задачи удаленной установки** (см. стр. 139) мастера развертывания защиты выберите параметр **Назначить установку инсталляционного пакета в групповых политиках Active Directory**.

3. На странице **Выбор учетных записей для доступа к устройствам** (см. стр. 140) 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 защиты 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 **Распространение инсталляционного пакета** (см. стр. 408).
3. Создайте задачу удаленной установки программы на подчиненных Серверах администрирования (см. стр. 316). 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.

kaspersky

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 **Активы (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:
   - **Установите пароль 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.....410

Сценарий: Развертывание программ "Лаборатории Касперского".....299

Сценарий: Мониторинг и отчеты.....496

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 при настройке удаленной установки программы

Вы можете включить параметр **Удалять несовместимые программы автоматически** во время настройки удаленной установки программы безопасности в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые программы перед установкой программы безопасности на управляемое устройство.

Инструкция: Удаление несовместимых программ перед установкой (см. стр. 140).

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.

Инструкция: Создание задачи (см. стр. 408).

Удаленная деинсталляция программ или обновлений программного обеспечения

Вы можете удаленно деинсталлировать программы или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

► *Чтобы удаленно деинсталлировать программы или обновления программного обеспечения:*

1. В главном окне программы перейдите к закладке **Активы (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**
7. Укажите, как клиентские устройства будут загружать утилиту удаления:
   - **С помощью Агента администрирования**
   - **Средствами операционной системы 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).

- **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 (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 (Агент администрирования не используется)**

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. 410).

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 323

Подготовка устройства под управлением Windows 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 **Отключить 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).

Используйте утилиту riprep для подготовки устройства под управлением Windows к удаленной установке. Чтобы скачать утилиту, перейдите по этой ссылке:
https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

Утилита подготовки устройства к удаленной установке не работает под управлением операционной системы Microsoft Windows XP Home Edition.

kaspersky

В этом разделе

Подготовка устройства под управлением Windows к удаленной установке в интерактивном режиме

► *Чтобы подготовить устройство под управлением Windows 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 под управлением Windows к удаленной установке в тихом режиме

► *Чтобы подготовить устройство под управлением Windows к удаленной установке в тихом 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` – запустить утилиту на выполнение в тихом 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 тихом 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).

kaspersky

Лицензирование программы

Этот раздел содержит информацию:

- Общие понятия, связанные с лицензированием Kaspersky Security Center
- Инструкция по управлению лицензиями управляемых программ "Лаборатории Касперского"

См. также:

В этом разделе

О лицензировании Kaspersky Security Center

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center.

В этом разделе

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать программу.

kaspersky

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 Linux следующими способами:

- при загрузке дистрибутива Агента администрирования с веб-серверов "Лаборатории Касперского";
- во время установки Агента администрирования для Linux;
- прочитав документ license.txt, входящий в комплект поставки Агента администрирования для Linux;
- прочитав документ license.txt в папке установки 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 лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center, предоставляемое вам на основании Лицензионного соглашения.

Объем предоставляемых услуг и срок использования программы зависят от лицензии, по которой используется 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 использовать программу по пробной лицензии только в течение одного пробного периода.

- *Коммерческая*

  Платная лицензия.

  По истечении срока коммерческой лицензии ключевые функции программы отключатся. Чтобы продолжить использование Kaspersky Security Center, вам нужно продлить срок действия коммерческой лицензии. По истечении срока действия коммерческой лицензии вы не сможете продолжать использовать программу и должны удалить его со своего устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывную защиту от угроз компьютерной безопасности.

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.

Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице https://www.kaspersky.ru/products-and-services-privacy-policy.

Политика конфиденциальности также доступна в офлайн-режиме.

- Вы можете ознакомиться с Политикой конфиденциальности перед установкой Kaspersky Security Center (см. стр. 85).
- Текст Политики конфиденциальности находится в файле license.txt в папке установки Kaspersky Security Center.
- Файл privacy_policy.txt доступен на управляемом устройстве в папке Агента администрирования.
- Вы можете распаковать файл privacy_policy.txt из дистрибутива Агента администрирования.

Варианты лицензирования Kaspersky Security Center

Kaspersky Security Center поставляется в составе программ "Лаборатории Касперского" для защиты корпоративных сетей. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

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".
- Выполнять удаленную установку программ "Лаборатории Касперского" и других программ сторонних производителей.
- 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 шифрованием данных, хранящихся на жестких дисках устройств с операционной системой Windows и съемных дисках.

- Управлять доступом пользователей к зашифрованным данным устройств с операционной системой Windows.
- 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.

О файле ключа

Активация сертифицированного программного изделия должна осуществляться только с использованием файла 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 предоставлении данных

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;
- 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:

- Информация об устройствах в сети организации получена путем опроса контроллеров домена Active Directory или Samba или путем опроса IP-диапазонов. Сервер администрирования самостоятельно получает данные или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Информация из Active Directory и Samba об организационных подразделениях, доменах, пользователях и группах. Сервер администрирования самостоятельно получает данные или их передает ему Агент администрирования, который выполняет роль точки распространения.
- Данные об управляемых устройствах. Агент администрирования передает от устройства Серверу администрирования перечисленные ниже данные. Пользователь вводит отображаемое имя и описание устройства в интерфейсе Kaspersky Security Center Web Console:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, имя и тип Windows-домена (для устройств, относящихся к Windows-домену), имя устройства в среде Windows (для устройств, относящихся к Windows-домену), 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: 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, под управлением которого находится устройство.
  - 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.
- Данные, полученные при запуске удаленной диагностики на управляемом устройстве: файлы трассировки, системная информация, сведения об установленных на устройстве программах "Лаборатории Касперского", файлы дампов, журналы событий, результаты запуска диагностических скриптов, полученные от Службы технической поддержки "Лаборатории Касперского".
- 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 Kaspersky Security Center Web Console.
- 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, данные о параметрах и задачах программы "Лаборатории Касперского", информация о лицензионных ключах, активном и резервном, 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".
- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.
- Настройки компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Настройки задач компонентов Kaspersky Security Center и управляемых программ "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает с устройства на Сервер администрирования следующую информацию:
  - Информация об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).
  - Данные о программах, установленных на управляемых устройствах (Реестр программ). Программы могут быть сопоставлены с информацией об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль программ.
- Пользовательские категории программ. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль программ. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Информация о шифровании устройств с операционной системой Windows и статусах шифрования. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования.
- Информация об ошибках шифрования данных на устройствах с операционной системой Windows, 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.
- 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 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.
- Информация о зашифрованных устройствах и статусе шифрования. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования.
- Информация об ошибках шифрования данных на устройствах. Шифрование выполняется функцией Шифрование данных программ "Лаборатории Касперского". Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в онлайн-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 о введенных кодах активации или файлах ключей. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center Web Console.
- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной телефон, пароль. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center Web Console. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные, необходимые для работы плагинов управляемых программ в Kaspersky Security Center 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 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 Web Console.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Информация о принятии пользователем условий юридических соглашений с "Лабораторией Касперского".

- Данные Сервера администрирования, которые Пользователь вводит в интерфейсе Kaspersky Security Center Web Console или в программном интерфейсе Kaspersky Security Center Open API.
- Любые данные, которые Пользователь вводит в интерфейсе Kaspersky Security Center Web Console.

Перечисленные выше данные могут попасть в Kaspersky Security Center следующими способами:

- Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- 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.
- Сервер администрирования самостоятельно получает информацию о сетевых устройствах или их передает ему Агент администрирования, который выполняет роль точки распространения.

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 дампов, файлы трассировки или файлы журналов компонентов Kaspersky Security Center содержат произвольные данные Сервера администрирования, Агента администрирования и Kaspersky Security Center Web Console. Эти файлы могут содержать персональные или прочие конфиденциальные данные. Файлы дампов, файлы трассировки или файлы журналов хранятся в открытой форме на устройствах. Файлы дампов, файлы трассировки или файлы журналов не передаются в "Лабораторию Касперского" автоматически, однако, администратор может передать эти файлы в "Лаборатории Касперского" вручную по запросу Службы технической поддержки для решения проблем в работе Kaspersky Security Center.

"Лаборатория Касперского" обеспечивает защиту всех полученных данных в соответствии с законодательством и применимыми правилами "Лаборатории Касперского". Данные передаются по безопасным каналам связи.

Переходя по ссылкам в Консоли администрирования или Kaspersky Security Center Web Console, Пользователь соглашается на автоматическую передачу следующих данных:

- код программы Kaspersky Security Center;
- версия программы Kaspersky Security Center;
- язык локализации программы 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.

kaspersky

Лицензирование управляемых программ "Лаборатории Касперского"

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:

Начало работы 78

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:

- Автоматическое распространение
- с помощью инсталляционного пакета управляемой программы;
- с помощью задачи добавления 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. Вы должны включить параметр **Распространять лицензионный ключ автоматически** для всех трех лицензионных ключей. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Linux. 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. 345), таким устройствам будет присвоен статус *Критический*.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 341)
- Автоматическое распространение лицензионного ключа (см. стр. 343)

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.

Добавление лицензионного ключа в инсталляционный пакет (см. стр. 138).

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.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 341)
- Распространение лицензионного ключа на клиентские устройства (на стр. 342)

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.

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.

kaspersky

См. также

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center Web Console позволяет распространить лицензионный ключ на клиентские устройства с помощью задачи *Распространение лицензионного ключа*.

Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 341).

► *Чтобы распространить лицензионный ключ на клиентские устройства:*

1. В главном окне программы перейдите к закладке **Активы (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 **Создать**.

   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.

kaspersky

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 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.

kaspersky

См. также

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 лицензионном 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 **Активы (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. 171).

См. также

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**.

Удаление лицензионного ключа из хранилища

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 ключ 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 Сервером администрирования.

      Откроется окно свойств Сервера администрирования.
   b. На вкладке **Общие** выберите раздел **Лицензионные ключи**.
   c. Если в открывшемся разделе отображается требуемый файл ключ 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 ключ 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 и нажмите на кнопку **Удалить**.

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить (см. стр. 341) удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

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.

► *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.

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 продления срока действия лицензии следуйте инструкциям.

   Срок действия лицензии продлен.

В Kaspersky Security Center 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:

kaspersky

Настройка программ "Лаборатории Касперского"

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 351

Настройка и распространение политик: подход, ориентированный на пользователя 353

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. 85)

- Установили Kaspersky Security Center Web Console (см. стр. 92)
- Основной сценарий установки Kaspersky Security Center завершен.
- Мастер первоначальной настройки (см. стр. 129) 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.

Настройка защиты сети состоит из следующих этапов:

1. 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. 351): ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

c. **Настройка задач для удаленного управления программами "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкция: Настройка групповой задачи обновления Kaspersky Endpoint Security (см. стр. 398).

   При необходимости создайте дополнительные задачи управления программами "Лаборатории Касперского", установленными на клиентских устройствах.

d. **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.

   Инструкция: Настройка количества событий в хранилище событий (см. стр. 165).

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. 468).

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

kaspersky

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.

Управление безопасностью, ориентированное на устройства (см. стр. 351), 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.

Управление безопасностью, ориентированное на пользователя (см. стр. 353), 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 проблемы 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. 360) 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. 466).

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.

kaspersky

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center (см. стр. 85) и Kaspersky Security Center Web Console (см. стр. 92). Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователя (см. стр. 353) как альтернативу или дополнительную возможность для подхода, ориентированного на устройства. Узнайте больше о двух подходах к управлению (см. стр. 351).

Этапы

Сценарий управления программами "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1. Настройка политик программ

   Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. стр. 367) 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 Linux – для клиентских устройств с операционной системой Linux.

   Kaspersky Endpoint Security для Windows – для клиентских устройств с операционной системой Windows.

   Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы.

   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 позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики (см. стр. 367).

2. Создание профилей политики (если требуется)

   Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики (см. стр. 360) 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, имеющим определенную конфигурацию программного обеспечения или имеющим заданные теги (см. стр. 285). Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *CentOS*, назначить его всем устройствам под управлением операционной системы CentOS, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы CentOS установленные программы "Лаборатории Касперского" будут управляться своим профилем политики.

   Инструкции:

- Создание профиля политики (см. стр. 377)
- Создание правила активации профиля политики (см. стр. 378)

2. 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.

   Инструкция: Принудительная синхронизация (см. стр. 373).

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:

Начало работы 78
Иерархия Серверов администрирования 52
Группы администрирования 56
Политики 58
Профили политик 59
О ролях пользователей 430
Сценарий: Настройка защиты сети 349

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.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center (см. стр. 85) и Kaspersky Security Center Web Console (см. стр. 92) и завершили основной сценарий установки. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства (см. стр. 351)

как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению (см. стр. 351).

Процесс

Сценарий управления программами "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. Настройка политик программ

   Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики 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.

   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. 357). Остальные незаблокированные параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. 359) позволяет эффективно управлять устройствами в группах администрирования.

   Инструкция: Создание политики (см. стр. 367).

2. Укажите пользователей в качестве владельцев устройств

   Назначьте управляемым устройствам соответствующие роли.

   Инструкция: Назначение пользователя владельцем устройства (см. стр. 451).

3. 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.

4. 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.

   Инструкция: Создание роли пользователя (см. стр. 464).

5. 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.

   Инструкция: Изменение области для роли пользователя (см. стр. 465).

6. Создание профиля политики

Создайте профиль политики (см. стр. 360) 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.

Инструкция: Создание профиля политики (см. стр. 377)

7. 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.

   Инструкция: Связь профилей политики с ролями (см. стр. 466).

8. Распространение политик и профилей политик на управляемые устройства

   По умолчанию синхронизация Kaspersky Security Center 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.

   Инструкция: Принудительная синхронизация (см. стр. 373).

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:

Начало работы 78

Иерархия Серверов администрирования 52

Группы администрирования 56

Политики 58

Профили политик 59

О ролях пользователей 430

Сценарий: Настройка защиты сети 349

kaspersky

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для программ "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

В этом разделе

См. также:

Сценарий: Настройка защиты сети 349

О политиках и профилях политик

Политика – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 56) и ее подгруппам. Вы можете установить несколько программ "Лаборатории Касперского" (см. стр. 37) 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:

Таблица 30. 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.
- 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 358

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (). В таблице ниже показаны состояния значка замка:

Таблица 31. Статусы значка замка

Состояние	Описание
Undefined	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*.
Enforce	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:

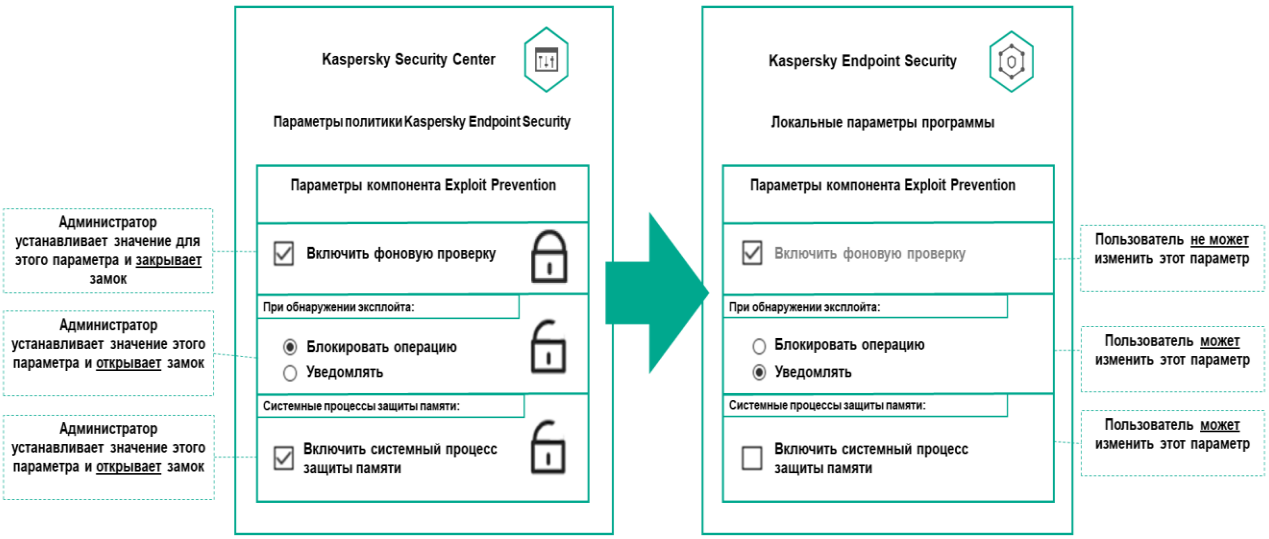
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров программы "Лаборатории Касперского" на управляемом устройстве.

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).



См. также:

Профили политик в иерархии политик.....360

Иерархия политик.....359

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

kaspersky

В этом разделе

Иерархия политик

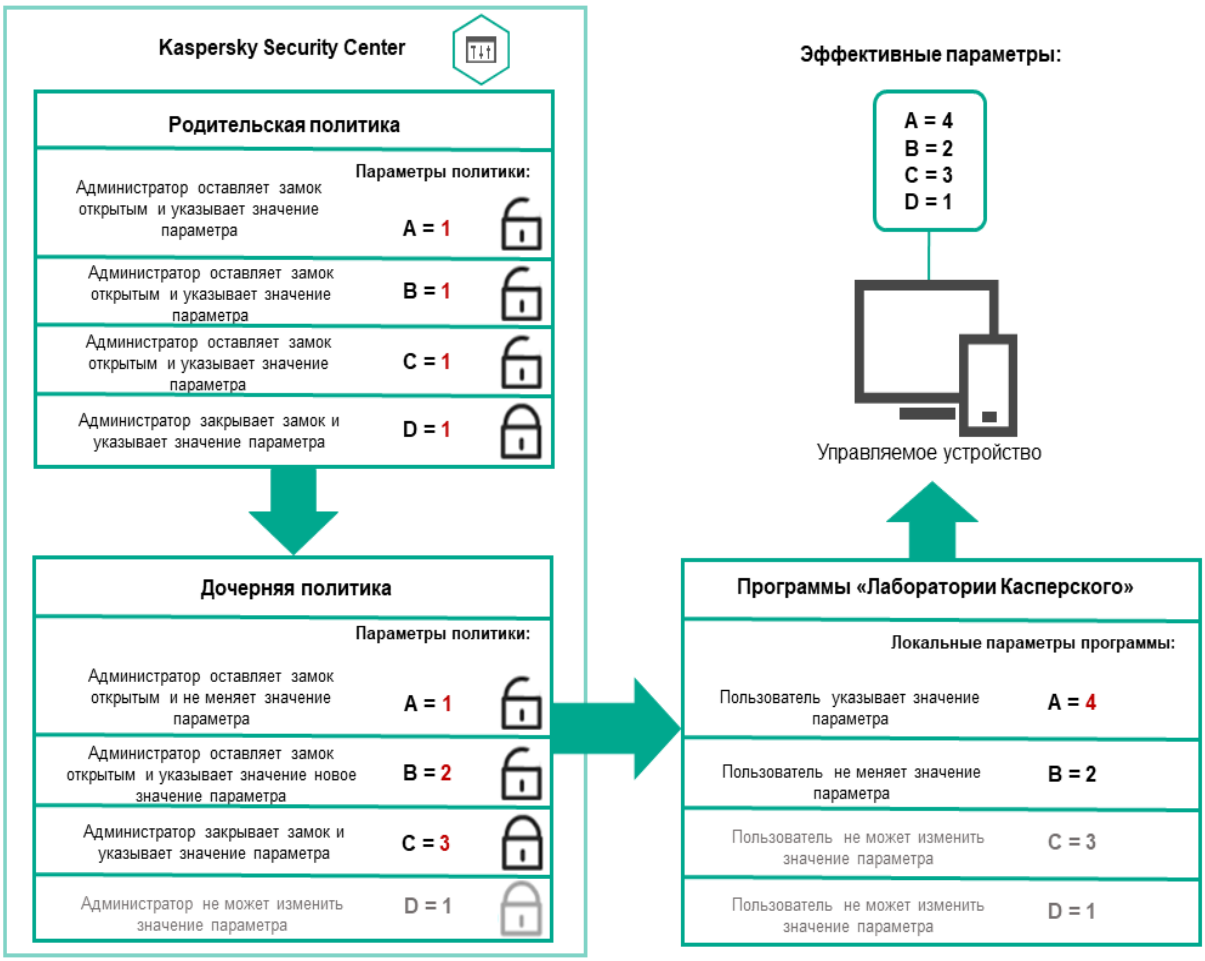
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования (см. стр. 56). 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.

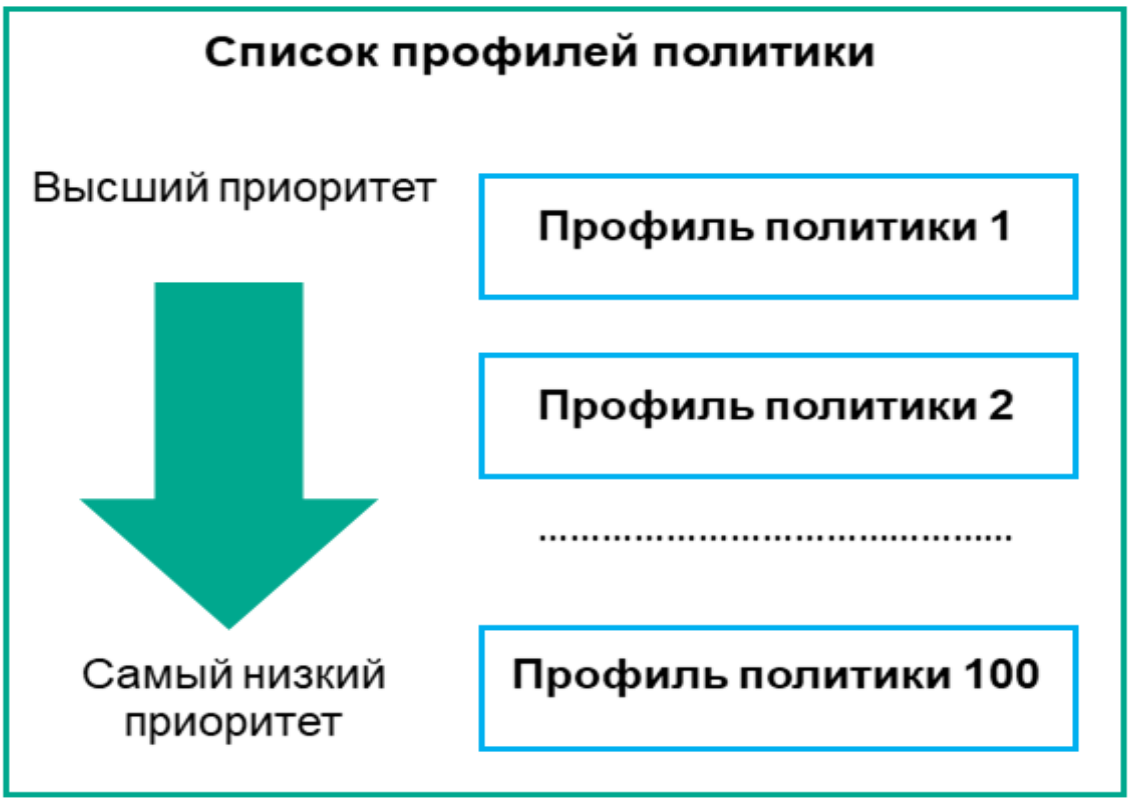
Политики одной и той же программы действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).



Профили политик в иерархии политик

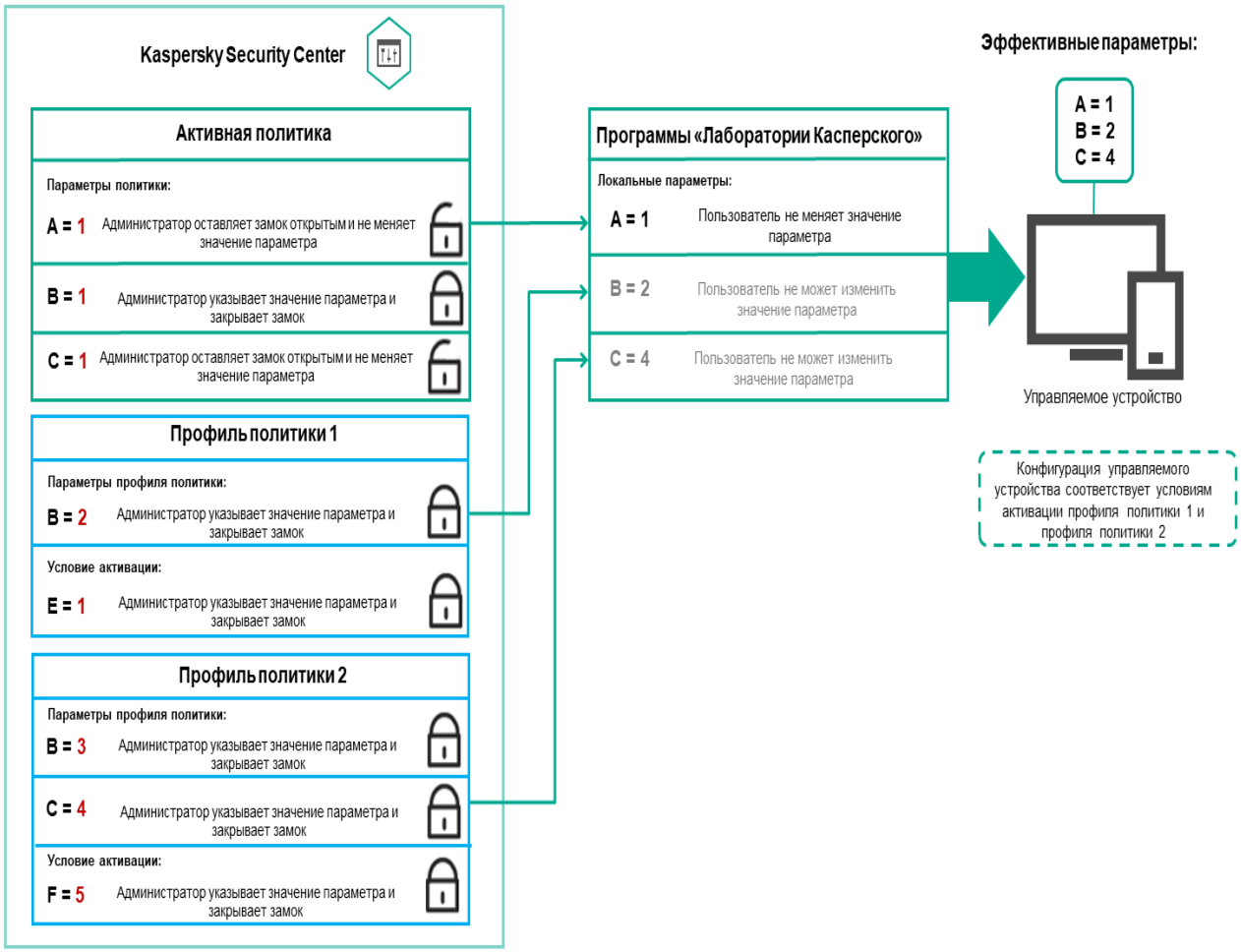
Профили политики имеют следующие условия назначения приоритета:

- 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).

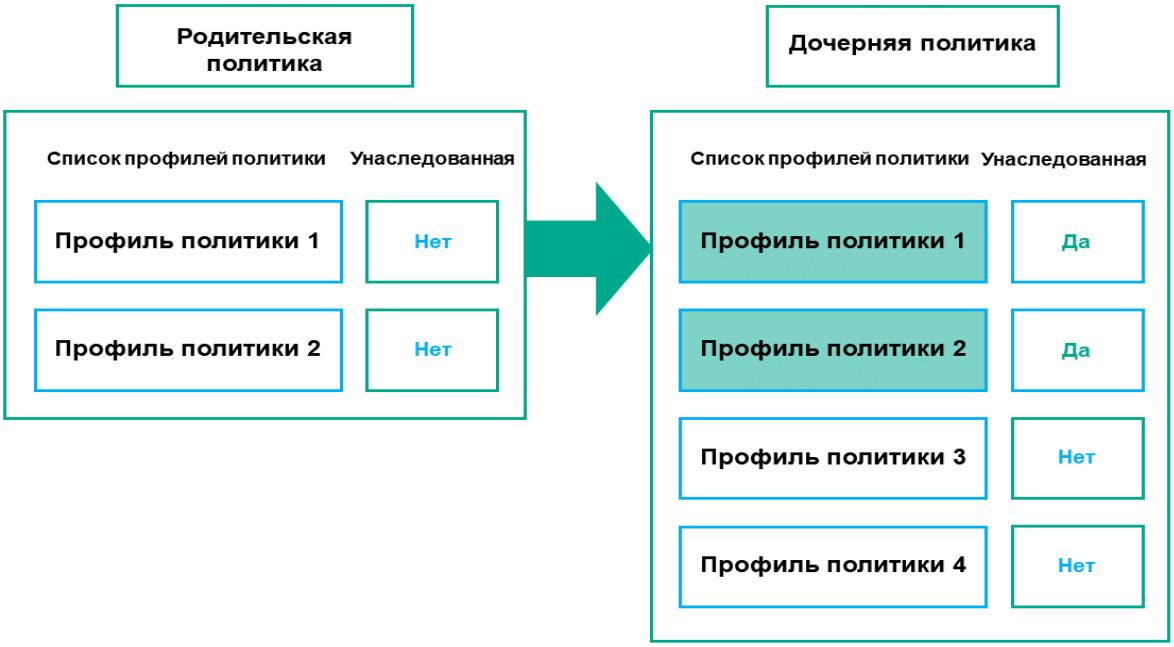


Профили политик в иерархии наследования

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.

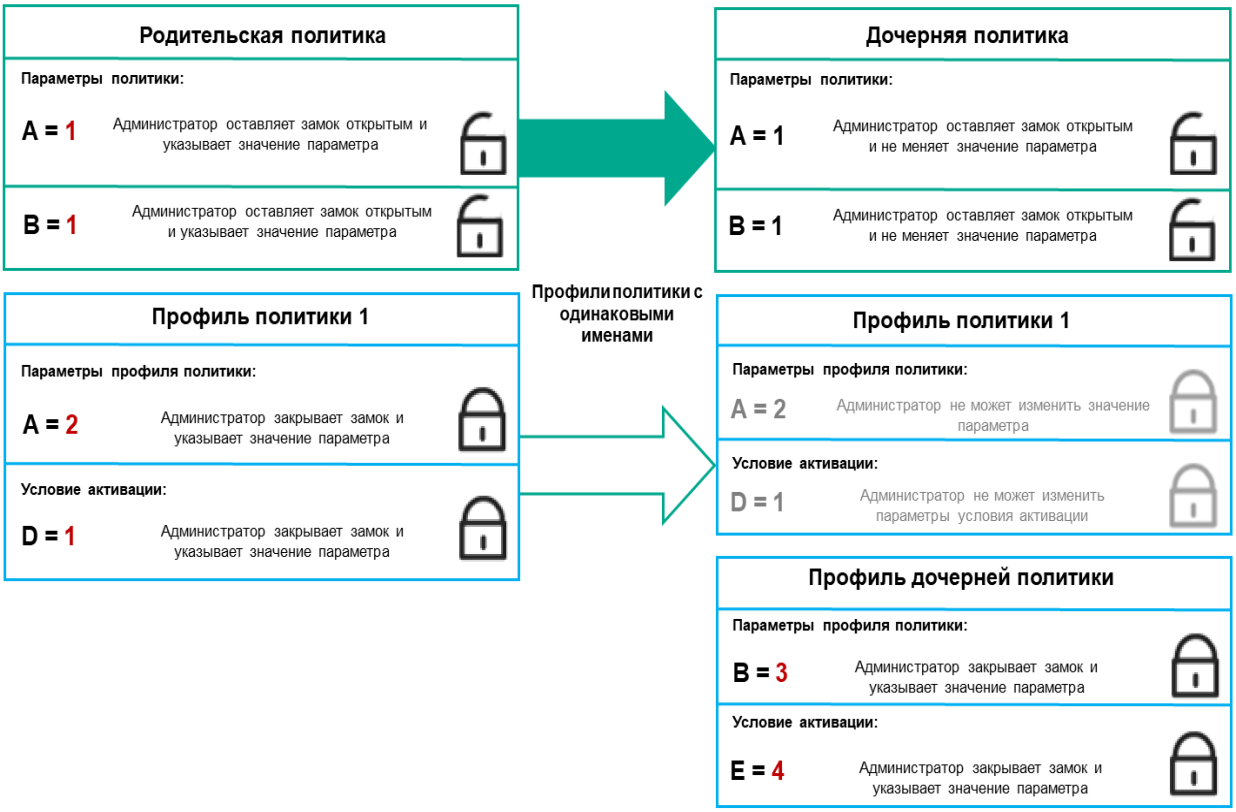
- Вы не можете изменить приоритет унаследованного профиля политики (см. рисунок ниже).



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 351

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.

kaspersky

См. также:

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 **Активы (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:

kaspersky

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 **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбрать программу**.
3. Выберите программу, для которой требуется создать политику.
4. Нажмите **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 **Параметры 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 **Параметры 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. 152)
   - Параметры политики Агента администрирования (см. стр. 382)
   - Онлайн-справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/219385.htm
   - Онлайн-справка Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/222859.htm

   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" 299

kaspersky

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**

    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.
  - **Форсировать наследование параметров дочерними политиками**

    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 закладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Предельный.**

  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**
  - **Хранить в журнале событий ОС на устройстве**
  - **Хранить в журнале событий ОС на Сервере администрирования**
- **Настройка событий**

  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. 575).

См. также:

Сценарий: Настройка защиты сети 349

Изменение политики

► *Чтобы изменить политику:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.
3. Укажите общие параметры (см. стр. 368) и параметры программы, для которой вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования (см. стр. 152)
   - Параметры политики Агента администрирования (см. стр. 382)
   - Онлайн-справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/219385.htm

- Онлайн-справка Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/222859.htm

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**.

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 **Форсировать наследование параметров дочерними политиками**, 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 359

Сценарий: Настройка защиты сети 349

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 **Активы (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 **Активная** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

См. также:

Сценарий: Настройка защиты сети 349

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 **Активы (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** вверху 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 **Активная** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

См. также:

Сценарий: Настройка защиты сети 349

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 как в Kaspersky Security Center Windows, так и в Kaspersky Security Center (см. стр. 372).

► *Чтобы экспортировать политику:*

1. В главном окне программы перейдите в раздел **Активы (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 **Экспорт** будет неактивна.
3. Нажмите на кнопку **Экспорт**.
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, ее параметры и профили политики (см. стр. 372).

► *Чтобы импортировать политику:*

1. В главном окне программы перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на кнопку **Импорт**.
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 **Готово**, 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)**.

Принудительная синхронизация

Несмотря на то, что Kaspersky Security Center автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору требуется точно знать, была ли выполнена синхронизация для определенного устройства в данный момент.

Синхронизация одного устройства

► *Чтобы осуществить принудительную синхронизацию между Сервером администрирования и управляемым устройством:*

1. В главном окне программы перейдите в раздел **Активы (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 **Активы (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. 272), 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 **Активы (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.

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 **Активы (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 100000.

► *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.

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 **Активы (Устройства)** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, 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 349

kaspersky

Управление профилями политик

В этом разделе описывается управление профилями политики и предоставляется информация о просмотре профилей политики, изменении приоритета профиля политики, создании профиля политики, копировании профиля политики, создании правила активации профиля политики и удалении профиля политики.

В этом разделе

Просмотр профилей политики

► *Чтобы просмотреть профили политики:*

1. В главном окне программы перейдите в раздел **Активы (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 349

Изменение приоритета профиля политики

► *Чтобы изменить приоритет профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 376).

   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.....360
Наследование политик и профилей политик 358
Сценарий: Настройка защиты сети 349

Создание профиля политики

► *Чтобы создать профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 376).

   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 **Параметры 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 **Параметры 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 351
Сценарий: Настройка защиты сети 349

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. 376).

   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 349

Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 376).

   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. 377).

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 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.

- **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 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:

- 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.

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 на закладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

► *Чтобы удалить профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 376).

   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 349

kaspersky

Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования:*

1. В главном окне программы перейдите в раздел **Активы (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 Linux и Windows, доступны различные параметры (см. стр. 388).

Общие

На этой вкладке 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.
  - **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.
  - **Форсировать наследование параметров дочерними политиками**

    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 вкладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на вкладке **Настройка событий**:

- **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). После того как вы нажмете на тип события, можно настроить параметры регистрации и уведомления о событиях, выбранных в списке. По умолчанию общие настройки уведомлений, указанные для всего Сервера администрирования, используются для всех типов событий. Однако можно изменить определенные параметры для заданных типов событий.

Например, в разделе **Предупреждение**, вы можете настроить тип события **Произошла проблема безопасности**. Такие события могут произойти, например, когда свободное место на диске точки распространения (см. стр. 62) меньше 2 ГБ (для установки программ и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошла проблема безопасности**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаружил инцидент, вы можете управлять этим инцидентом, используя параметры управляемого устройства (см. стр. 239).

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. 471).

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 Linux). 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.

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.

- **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 информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Подключения.

Раздел **Подключения** включает три вложенных раздела:

- **Сеть**
- **Профили соединений**
- **Расписание соединений.**

В разделе **Сеть** 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) 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.

- **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 управляемое устройство подключалось к прокси-серверу KSN через UDP-порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порта** 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.

В подразделе **Профили соединений** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен. Параметры раздела **Профили соединений** доступны только для устройств под управлением Windows:

- **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**

Профили подключения поддерживаются только для устройств под управлением Windows.

Вы можете 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.
- **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. 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 разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Zeroconf**
- **IP-диапазоны**

  Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по ссылке **Настроить расписание опроса**.

  Если 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.

- **Контроллеры домена**

Параметры сети для точек распространения

В разделе **Параметры сети для точек распространения** вы можете указать 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 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 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/KPSN непосредственно через интернет**

  Точка распространения пересылает KSN запросы от управляемых устройств облачной-службе KSN или KPSN. Запросы KSN, сгенерированные на самой точке распространения, также отправляются непосредственно в KSN Cloud или KPSN.

- **Порт**

  Номер TCP-порта, который управляемые устройства используют для подключения к прокси-серверу KSN. По умолчанию установлен порт 13111.

- **UDP-порт**

  Чтобы управляемое устройство подключалось к прокси-серверу KSN через UDP-

порт, установите флажок **Использовать UDP-порт** и в поле **Номер UDP-порта** 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, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского" (см. стр. 490).

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Сравнение параметров политики Агента администрирования по операционным системам388В этом разделе

Сравнение параметров политики Агента администрирования по операционным системам.....388

Сравнение параметров политики Агента администрирования по операционным системам

В таблице ниже показано, какие параметры политики Агента администрирования можно использовать для настройки Агента администрирования для конкретной операционной системы (см. стр. 382).

Таблица 32. Параметры политики Агента администрирования: сравнение по операционным системам

Раздел Политики	Linux	Windows
Общие	✓	✓
Настройка событий	✓	✓
Параметры	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Программа может получать расширенные данные политики на устройстве**	✓

Раздел Политики	Linux	Windows
Хранилища	✓ Доступны следующие параметры: • **Информация об установленных программах** • **Информация о реестре оборудования**	✓
Подключения → Сеть	✓ Кроме параметра **Открывать порты Агента администрирования в брандмауэре Microsoft Windows**.	✓
Подключения → Профили соединений	—	✓
Подключения → Расписание соединений	✓	✓
Опрос сети точками распространения.	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры домена**	✓ Доступны следующие параметры: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры домена**
Параметры сети для точек распространения	✓	✓
Прокси-сервер KSN (точки распространения)	✓	✓
Обновления (точки распространения)	✓	✓
История ревизий	✓	✓

kaspersky

Использование Агента администрирования для Windows и Linux: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы (см. стр. 234). В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows и Linux.

Таблица 33. Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux
Установка		
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами (см. стр. 212).	✓	✓
Установка программ с помощью сторонних средств удаленной установки программ	✓	✓
Установка вручную с помощью запуска инсталляторов программ на устройствах	✓	✓
Установка Агента администрирования в тихом режиме (см. стр. 219).	✓	✓
Установка Агента администрирования в тихом режиме (см. стр. 230).	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	✓	—
Автоматическое распространение ключа	✓	✓
Принудительная синхронизация	✓	✓
Точка распространения		
Использование точки распространения (см. стр. 202).	✓	✓
Автоматическое назначение точек распределения (см. стр. 204).	✓	✓ Без использования Network Location Awareness (NLA).
Офлайн-модель получения обновлений	✓	✓

Функция Агента администрирования	Windows	Linux
Опрос сети	✓ • Опрос IP-диапазонов • Опрос сети Windows • Опрос Active Directory	✓ • Опрос IP-диапазонов • Опрос Zeroconf • Опрос контроллеров домена
Запуск службы прокси-сервер KSN на стороне точки распространения	✓	✓
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓	✓
Принудительная установка программ	✓	С ограничением: нельзя выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.
Использовать в качестве push-сервера	✓	✓
Работа с программами сторонних производителей		
Удаленная установка программ на устройства (см. стр. 216).	✓	—
Обновления программного обеспечения.	✓	—
Настройка обновлений операционной системы в политике Агента администрирования.	✓	—
Просмотр информации об уязвимостях в программах.	✓	—
Поиск уязвимостей в программах.	✓	—
Инвентаризация программного обеспечения, установленного на устройствах.	✓	✓
Виртуальные машины		
Установка Агента администрирования на виртуальные машины (см. стр. 225).	✓	✓
Оптимизация параметров для VDI (см. стр. 225).	✓	✓

Функция Агента администрирования	Windows	Linux
Поддержка динамических виртуальных машин (см. стр. 226).	✓	✓
Другое		
Аудит действий на удаленном клиентском устройстве с помощью совместного доступа к рабочему столу Windows	✓	—
Мониторинг состояния антивирусной защиты	✓	✓
Управление перезагрузкой устройств	✓	—
Поддержка отката файловой системы (см. стр. 227).	✓	✓
Использование Агента администрирования в качестве шлюза соединений	✓	✓
Менеджер соединений	✓	✓
Переключение Агента администрирования с одного Сервера администрирования на другой (автоматически по сетевому местоположению)	✓	—
Проверка соединения клиентского устройства с Сервером администрирования. Утилита klnagchk	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	—
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓

См. также:

Развертывание Агента администрирования и программы безопасности 209

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:

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/12.0/ru-RU/177936.htm.

► *Чтобы задать рекомендуемые параметры KSN:*

1. В главном окне программы перейдите в раздел **Активы (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 KPSN), так и у третьих сторон (при использовании KPSN).
6. Нажмите на кнопку **ОК**.

Рекомендованные параметры KSN настроены.

См. также:

kaspersky

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/12.0/ru-RU/176738.htm.

► *Чтобы проверить список сетей:*

1. В главном окне программы перейдите в раздел **Активы (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 349

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 политики приведено в документации Kaspersky Endpoint Security для Windows. https://support.kaspersky.com/KESWin/12.0/ru-RU/176733.htm.

► *Чтобы выключить проверку сетевых дисков:*

1. В главном окне программы перейдите в раздел **Активы (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 → 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 349

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 **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на политику Kaspersky Endpoint Security для Windows.

   Откроется окно свойств выбранной политики.

3. **В свойствах 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 349

kaspersky

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 политики приведено в документации Kaspersky Endpoint Security для Windows. https://support.kaspersky.com/KESWin/12.0/ru-RU/178492.htm.

► *Чтобы задать рекомендуемые параметры интерфейса:*

1. В главном окне программы перейдите в раздел **Активы (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 349

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 **Активы (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 вкладку **Настройка событий**.
4. В разделе **Критический** нажмите на кнопку **Добавить событие** и установите флажок только рядом со следующим событием:
   - *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 событие** 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 событие** и установите флажки только рядом со следующими событиями:
   - *Самозащита программы выключена.*
   - *Компоненты защиты выключены.*
   - *Недопустимый резервный ключ.*
   - *Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (на основе локальных параметров).*

- *Обнаружено легальное ПО, которое может быть использовано злоумышленниками для нанесения вреда компьютеру или персональным данным (KSN).*
- *Объект удален.*
- *Объект вылечен.*
- *Пользователь отказался от политики шифрования.*
- *Файл восстановлен администратором из карантина на сервере Kaspersky Anti Targeted Attack Platform.*
- *Файл помещен администратором на карантин на сервере Kaspersky Anti Targeted Attack Platform.*
- *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 событие** и установите флажки только рядом со следующими событиями:
    - *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 349

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 349

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.

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. 400).

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. 400). 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 (KPSN) 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 Kaspersky Private Security Network в разделе **KSN Proxy settings** окна свойств Сервера администрирования (см. стр. 400).

Программа предлагает присоединиться к KSN во время работы мастера первоначальной настройки (см. стр. 133). Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с программой (см. стр. 402).

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. 171). 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-сервера KSN** окна свойств Сервера администрирования (см. стр. 400).

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 KSN:*

1. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **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 KPSN, переведите переключатель в положение **Использовать Kaspersky Private Security Network [Включено]** и нажмите на кнопку **Файл с параметрами прокси-сервера KPSN**, чтобы загрузить параметры KPSN (файлы с расширениями pkcs7 и pem). После загрузки параметров в интерфейсе отображаются наименование провайдера, контакты провайдера и дата создания файла с параметрами KPSN.

   При переводе переключателя в положение **Использовать Kaspersky Private Security Network [Включено]** появится сообщение с подробной информацией о KPSN.

   KPSN поддерживают следующие программы "Лаборатории Касперского":

   - Kaspersky Security Center
   - Kaspersky Endpoint Security для Linux
   - Kaspersky Endpoint Security для Windows

   Если вы включите KPSN в Kaspersky Security Center, эти программы получат об этом информацию о поддержке KPSN. В окне свойств программы в подразделе **Kaspersky Security Network** раздела **Продвинутая защита** отображается поставщик KSN: KSN или KPSN.

   > Kaspersky Security Center не отправляет статистику Kaspersky Security Network, если настроен KPSN в окне свойств Сервера администрирования в разделе **Параметры прокси-сервера KSN**.

5. Установите флажок **Игнорировать параметры прокси-сервера для подключения к KPSN**, если параметры прокси-сервера настроены в свойствах Сервера администрирования, но ваша архитектура сети требует, чтобы вы использовали KPSN напрямую. В противном случае запрос от управляемой программы не будет передан в KPSN.
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, выберите параметр **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. 258).
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 **Прокси-сервер KSN**, включите параметр **Включить прокси-сервер KSN на стороне точки распространения** и параметр **Доступ к облачной службе KSN/KPSN непосредственно через интернет**.
6. Нажмите на кнопку **ОК**.

Точка распространения будет исполнять роль прокси-сервера KSN.

> Обратите внимание, что точка распространения не поддерживает проверку подлинности управляемого устройства по протоколу NTLM.

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 вкладке **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 вкладке **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 один из этих переключателей выключен, клиентские устройства не будут передавать результаты установки патчей в "Лабораторию Касперского".

   Если вы используете KPSN, переведите переключатель в положение **Использовать Kaspersky Private 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 вкладке **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.

kaspersky

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN (см. стр. 403). 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 **Обновление Положения 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 (см. стр. 403) 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 Kaspersky Security Network (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 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.

► *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.

kaspersky

Управление задачами

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

В этом разделе

См. также:

Сценарий: Настройка защиты сети 349

О задачах

Kaspersky Security Center управляет работой программ безопасности "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 Web Console, только если для этой программы установлен плагин управления на сервере Kaspersky Security Center 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 с помощью Kaspersky Security Center Web Console, 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.

Область задачи

Область задачи (см. стр. 406) – 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) 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:

Управление задачами 406

Создание задачи

► *Чтобы создать задачу:*

1. В главном окне программы перейдите к закладке **Активы (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:

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 **Активы (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:

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center.

► *Чтобы просмотреть список задач,*

В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которыми они относятся. Например, задача *Удаленная установка программы* относится к Серверу администрирования, а задача *Обновление* относится к Kaspersky Endpoint Security.

► *Чтобы просмотреть свойства задачи,*

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными закладками (см. стр. 410). Например, **Тип задачи** отображается на закладке **Общие**, а расписание задачи на закладке **Расписание**.

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).
  - **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 *Обновление*.

- **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.

- **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 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:
  - **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 устройства после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

- **Выключать устройства 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:**
    - **Хранить в базе данных Сервера 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 системном журнале событий каждого клиентского устройства.

По умолчанию параметр выключен.

- **Хранить в журнале событий ОС на Сервере администрирования**

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в системном журнале событий операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранить 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" 299

Экспорт задачи

Kaspersky Security Center позволяет сохранить задачу и ее параметры в файл KLT. Вы можете использовать файл KLT для импорта сохраненной задачи как в Kaspersky Security Center Windows, так и в Kaspersky Security Center (см. стр. 416).

► *Чтобы экспортировать задачу:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.
2. Установите флажок рядом с задачей, которую вы хотите экспортировать.

   Невозможно экспортировать несколько задач одновременно. Если вы выберете несколько задач, кнопка **Экспорт** будет неактивна. Задачи Сервера администрирования и локальные задачи также недоступны для экспорта.
3. Нажмите на кнопку **Экспорт**.
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. 416) и ее параметры.

► *Чтобы импортировать задачу:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Импорт**.
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 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 **Активы (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, которые в настоящее время действительны в вашей системе. 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 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:

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, выполните следующие действия:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

См. также:

Сценарий: Настройка защиты сети 349

Теги программ

В этом разделе описаны теги программ, приведены инструкции по их созданию и изменению, а также по назначению тегов сторонним программам.

См. также:

Теги устройств 285
Сценарий: Управление программами 588

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. 272).

Например, можно создать тег [Браузеры] и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

См. также:

Сценарий: Управление программами 588
Сценарий: Обнаружение устройств в сети 174

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:

Сценарий: Управление программами 588
Сценарий: Обнаружение устройств в сети 174

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 588
Сценарий: Обнаружение устройств в сети 174

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 588
Сценарий: Обнаружение устройств в сети 174

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. 423).

См. также:

Сценарий: Управление программами 588
Сценарий: Обнаружение устройств в сети 174

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 **ОК**.

Выбранный тег программы удален. Удаленный тег автоматически снимается со всех программ, которым он был назначен.

См. также:

Сценарий: Управление программами 588
Сценарий: Обнаружение устройств в сети 174

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств

В компоненте Контроль устройств политики Kaspersky Endpoint Security 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.

kaspersky

Вы можете предоставить автономный доступ к внешнему устройству, заблокированному Контролем устройств, только если в параметрах политики Kaspersky Endpoint Security включен параметр **Разрешать запрашивать временный доступ** в разделе **Параметры программы → Контроль безопасности → Контроль устройств**.

Предоставление автономного доступа к внешнему устройству, заблокированному компонентом Контроль устройств, включает в себя следующие этапы:

1. В диалоговом окне Kaspersky Endpoint Security 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 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 **Активы (Устройства) → Управляемые устройства**.

   Отобразится список управляемых устройств.
2. В этом списке выберите пользовательское устройство, которое запрашивает доступ к внешнему устройству, заблокированному компонентом Контроль устройств.

   Можно выбрать только одно устройство.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (•••) и нажмите 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 получили от пользователя, а затем 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**.
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, пользователь получает временный доступ к заблокированному устройству на определенный период.

См. также:

Сценарий: Настройка защиты сети 349

Использование утилиты klscflag для открытия порта 13291

Порт 13291 на Сервере администрирования используется для приема подключений от Консоли администрирования на базе MMC. На компьютерах, с операционными системами отличных от Windows, этот порт по умолчанию закрыт.

Если вы хотите разрешить подключение к Консоли администрирования на основе консоли Microsoft Management Console (MMC) или использовать утилиту klakaut, вы можете открыть этот порт с помощью утилиты klscflag. Обратите внимание, что функциональность Консоли администрирования на базе MMC снижается при ее подключении к Kaspersky Security Center. Рекомендуется использовать Kaspersky Security Center Web Console для подключения к Kaspersky Security Center.

Утилита изменяет значение параметра KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Рекомендуется использовать Web Console для подключения к Kaspersky Security Center.

► *Чтобы открыть порт 13291:*

1. Выполните следующую команду в командной строке:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
\"SS_SETTINGS\";"
```

2. Перезапустите службу Сервера администрирования Kaspersky Security Center, выполнив следующую команду:

```
$ sudo systemctl restart kladminserver_srv
```

Порт 13291 открыт.

► *Чтобы проверить, был ли успешно открыт порт 13291:*

Выполните следующую команду в командной строке:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SET-
TINGS\";"
```

Эта команда возвращает следующий результат:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

Значение `true` означает, что порт открыт. В противном случае отображается значение `false`.

См. также:

Порты, используемые программой Kaspersky Security Center Web Console 49

Порты, используемые Kaspersky Security Center 45

Разделение доступа к функциям программы по пользовательским ролям

По умолчанию пользователи, входящие в группу "Администраторы" на защищаемом сервере, имеют доступ ко всем функциям Kaspersky Security Center.

Пользователи, которые имеют доступ к функции **Изменение прав** Kaspersky Security Center, могут предоставлять доступ к функциям Kaspersky Security Center другим пользователям, зарегистрированным на защищаемом сервере или входящим в домен.

Если пользователь не зарегистрирован в списке пользователей Kaspersky Security Center, он не может открыть Консоль Kaspersky Security Center.

Вы можете выбрать для пользователя или группы пользователей Kaspersky Security Center один из следующих предустановленных уровней доступа к функциям Kaspersky Security Center:

- **Полный контроль** – доступ ко всем функциям программы: возможность просматривать и изменять общие параметры работы Kaspersky Security Center, параметры работы компонентов Kaspersky Security Center, права пользователей Kaspersky Security Center, а также просматривать статистику работы Kaspersky Security Center.
- **Изменение** – доступ ко всем функциям программы, кроме изменения прав пользователей: возможность просматривать и изменять общие параметры работы Kaspersky Security Center, параметры работы компонентов Kaspersky Security Center, а также просматривать статистику работы Kaspersky Security Center и права пользователей Kaspersky Security Center.
- **Чтение** – возможность просматривать общие параметры работы Kaspersky Security Center, параметры работы компонентов Kaspersky Security Center, статистику работы Kaspersky Security Center и права пользователей Kaspersky Security Center.

Также вы можете выполнять расширенную настройку прав доступа: разрешать или запрещать доступ к отдельным функциям Kaspersky Security Center.

Если вы вручную настроили права доступа для пользователя или группы, то для этого пользователя или группы установлен уровень доступа **Особые разрешения**.

Таблица 34. Права доступа к функциям Kaspersky Security Center

Права доступа	Описание
Управление задачами	Возможность запускать / останавливать / приостанавливать / возобновлять задачи Kaspersky Security Center.
Создание и удаление задач	Возможность создавать и удалять задачи проверки по требованию.

Права доступа	Описание
Изменение параметров	Возможности: • просматривать и изменять общие параметры работы Kaspersky Security Center; • импортировать из конфигурационного файла и экспортировать в конфигурационный файл параметры работы Kaspersky Security Center; • просматривать и изменять параметры задач; • просматривать и изменять параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Чтение параметров	Возможности: • просматривать общие параметры работы Kaspersky Security Center и параметры задач; • экспортировать в конфигурационный файл параметры работы Kaspersky Security Center; • просматривать параметры журналов выполнения задач, журнала системного аудита и уведомлений.
Управление хранилищами	Возможности: • помещать объекты на карантин; • удалять объекты из карантина и резервного хранилища; • восстанавливать объекты из карантина и резервного хранилища.
Управление журналами	Возможность удалять журналы выполнения задач и очищать журнал системного аудита.
Чтение журналов	Возможность просматривать события в журналах выполнения задач и журнале системного аудита.
Чтение статистики	Возможность просматривать статистику работы каждой задачи Kaspersky Security Center.
Лицензирование программы	Возможность активировать и деактивировать Kaspersky Security Center.
Чтение прав	Возможность просматривать список пользователей Kaspersky Security Center и права доступа каждого пользователя.
Изменение прав	Возможности: • изменять список пользователей, имеющих доступ к управлению программой; • изменять права доступа пользователей к функциям Kaspersky Security Center.

kaspersky

Управление пользователями и ролями 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:

Сценарий: Настройка защиты сети 349

Об учетных записях пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами

безопасности. Программа поддерживает два типа учетных записей:

- Учетные записи сотрудников организации. Сервер администрирования получает данные об учетных записях этих локальных пользователей при опросе сети организации.
- Учетные записи внутренних пользователей Kaspersky Security Center. Вы можете создавать учетные записи внутренних пользователей на портале. Эти учетные записи используются только в Kaspersky Security Center.

► Чтобы просмотреть таблицы учетных записей пользователей и групп безопасности:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи и группы**.
2. Перейдите на вкладку **Пользователи** или **Группы**.

Откроется таблица пользователей или групп безопасности. Если вы хотите просмотреть таблицу только с учетными записями внутренних пользователей или групп, установите в фильтре **Подтип** критерий **Внутренний** или **Локальный**.

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. 444).

Если вы управляете устройствами с помощью иерархии Серверов администрирования, в которую входят виртуальные Серверы администрирования, обратите внимание, что вы можете создавать, изменять и удалять пользовательские роли только на физическом Сервере администрирования. Затем вы можете распространить пользовательские роли на подчиненные Серверы администрирования, в том числе виртуальные Серверы.

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.

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.

kaspersky

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 349

kaspersky

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. 432) для пользователей Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей (см. стр. 430) 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. 441) пользователей с уже настроенным набором прав или создавать роли (см. стр. 464) и самостоятельно настраивать необходимые права.

В этом разделе

См. также:

Сценарий: Настройка защиты сети 349

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: Базовая функциональность**.

Таблица 35. 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**. • Удаление устройства из состава группы администрирования: **Запись**. • Добавление группы администрирования в другую группу администрирования: **Запись**. • 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.

Общий функционал: **Общие функции**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Запись**, **Выполнение действий над выборками устройств**. • Получение мобильного протокола пользовательского сертификата (LWNGT): **Чтение**. • Установка мобильного протокола пользовательского сертификата (LWNGT): **Запись**. • Получить список сетей, определенных NLA: **Чтение**. • Добавить, изменить или удалить список сетей, определенных NLA: **Запись**. • Просмотр списка контроля доступа групп: **Чтение**. • Просмотрите журнал событий Kaspersky Event Log: **Чтение**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка программ на подчиненные Серверы администрирования.	• Отчет о состоянии защиты. • Отчет об угрозах. • Отчет о наиболее заражаемых устройствах. • Отчет о статусе антивирусных баз. • Отчет об ошибках. • Отчет о сетевых атаках. • Сводный отчет о программах для защиты периметра. • Сводный отчет о типах установленных программ. • Отчет о пользователях зараженных устройств. • Отчет об проблемах безопасности. • Отчет о событиях. • Отчет о работе точек распространения. • Отчет о подчиненных Серверах администрирования. • Отчет о событиях Контроля устройств. • Отчет о запрещенных программах. • Отчет о работе Веб-Контроля. • Отчет о статусе шифрования управляемых устройств. • Отчет о статусе шифрования запоминающих устройств. • Отчет о правах доступа к зашифрованным дискам. • Отчет об ошибках шифрования файлов. • Отчет о блокировании доступа	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
				к зашифрованным файлам. • Отчет об эффективных правах пользователя. • Отчет о правах.	
Общие функции: **Удаление объектов.**	• **Чтение.** • **Запись.**	• Просмотр удаленных объектов в корзине: **Чтение**. • Удаление объектов из корзины: **Запись**.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: **Обработка событий.**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Запись.**	• Изменение параметров регистрации событий: **Изменение параметров записи событий в журнал событий**. • Изменение параметров уведомления о событиях: **Изменение параметров уведомления о событиях**. • Удаление событий: **Удаление событий**	Отсутствует.	Отсутствует.	Параметры: • Максимальное количество событий, хранящихся в базе данных. • Период хранения событий удаленных устройств.

Общие функции: **Операции с Сервером администрирования.**	• **Чтение.** • **Запись.** • **Выполнение.** • **Изменение списков ACL объекта.** • **Выполнение действий над выборками устройств.**	• Изменение портов Сервера администрирования для подключения Агента администрирования: **Запись**. • Изменение портов прокси-сервера активации, запущенного на Сервере администрирования: **Запись**. • Изменение портов прокси-сервера активации для мобильных устройств, запускаемых на Сервере администрирования: **Запись**. • Изменение портов Веб-сервера для распространения автономных пакетов: **Запись**. • Изменение портов Веб-сервера для распространения iOS MDM-профилей: **Запись**. • Изменение SSL-портов Сервера администрирования для подключения с помощью Kaspersky Security Center Web Console: **Запись**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Запись**.	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
		• Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Запись**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Запись**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Запись**.			
Общие функции: **Развертывание программ "Лаборатории Касперского".**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского"**.	Отсутствует.	• Отчет об использовании лицензионных ключей виртуальным Сервером администрирования. • Отчет о версиях программ "Лаборатории Касперского". • Отчет о несовместимых программах. • Отчет о версиях обновлений модулей программ "Лаборатории Касперского". • Отчет о развертывании защиты.	Инсталляционный пакет: "Лаборатория Касперского".

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: **Управление лицензионными ключами.**	• **Экспорт файл ключа.** • **Запись.**	• Экспорт файл ключа: **Экспорт файл ключа**. • Изменение параметров лицензионного ключа Сервера администрирования: **Запись**.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: **Управление отчетами.**	• **Чтение.** • **Запись.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • 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 управления доступом объектов**. • Управление ролями пользователей: **Изменение списков управления доступом объектов**. • Управление внутренними пользователями: **Изменение списков управления доступом объектов**. • Управление группами безопасности: **Изменение списков управления доступом объектов**. • Управление псевдонимами: **Изменение списков управления доступом объектов.**	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.** • **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Получение списка виртуальных Серверов администрирования: **Чтение**. • Получение информации о виртуальном Сервере администрирования: **Чтение**. • Создание, обновление или удаление виртуального Сервера администрирования: **Управление виртуальными Серверами администрирования**. • Перемещение виртуального Сервера администрирования в другую группу: **Управление виртуальными Серверами администрирования**. • Установка прав доступа к виртуальному Серверу администрирования: **Управление виртуальными Серверами администрирования**.	Отсутствует.	Отсутствует.	Отсутствует.
Общие функции: **Управление ключами шифрования**	**Запись.**	Импорт ключей шифрования: **Запись**.	Отсутствует.	Отсутствует.	Отсутствует.

kaspersky

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям программы.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных пользовательских ролей, доступных в Kaspersky Security Center, можно связать с определенными должностями, например, **Аудитор**, **Специалист по безопасности**, **Контролер**. 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 36. 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.

Возможности функциональной области **Управление мобильными устройствами: Общие** и **Управление системой** недоступны в Kaspersky Security Center. Пользователь с ролями **Администратор Системного администрирования/Оператор** и **Администратор управления мобильными устройствами/Оператор** имеют права доступа только в функциональной области **Общий функционал**: **Базовая функциональность**.

Таблица 37. Права предопределенных ролей пользователей

Роль	Описание
Администратор Сервера администрирования	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Обработка событий.** • **Иерархия Серверов администрирования** • **виртуальные Серверы администрирования;** Предоставляет права на **Чтение** и **Запись** в области **Общий функционал: Управление ключами шифрования.**

Роль	Описание
Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **виртуальные Серверы администрирования;**
Аудитор	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Доступ к объектам независимо от их списков ACL.** • **Удаленные объекты.** • **Управление отчетами.** Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Администратор установки программ	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание программ "Лаборатории Касперского".** • **Управление лицензионными ключами.** Предоставляет права на **Чтение** и **Выполнение в следующей** функциональной области **Базовая функциональность: Виртуальные Серверы администрирования.**
Оператор установки программ	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание программ "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области)**.** • **виртуальные Серверы администрирования;**
Роль IRP-службы	Предоставляет права на **Запись** в **функциональной области Общие функции: Управление** группами администрирования. Предоставляет права на **Чтение** в функциональной области **Общий функционал: Базовая функциональность**.
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общий функционал: Общие функции** • Область Kaspersky Endpoint Security, включая все функции. 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: • **Общий функционал: Общие функции** • Область Kaspersky Endpoint Security, включая все функции.

Роль	Описание
Главный администратор	Разрешает все операции в функциональных областях, *за исключением* следующих областей: **Общий функционал**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** 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:
	• **Общие функции**:
	  • **Базовая функциональность.**
	  • **Удаленные объекты.**
	  • **Операции с Сервером администрирования.**
	  • **Развертывание программ "Лаборатории Касперского".**
	  • **виртуальные Серверы администрирования;**
	• Область Kaspersky Endpoint Security, включая все функции.

Администратор управления мобильными устройствами	Разрешает все операции в области **Общий функционал: функциональная область Базовая функциональность**.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет права на **Чтение**, **Запись**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой: Подключения.** 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: 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.** Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Роли служб	

Роль	Описание
Автоматическое реагирование на угрозы	Предоставляет право реагировать на угрозы.

Назначение прав доступа к набору объектов

В дополнение к назначению прав доступа на уровне сервера, вы можете настроить доступ к конкретным объектам, например, к требуемой задаче (см. стр. 432). 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:
   - **Активы (Устройства) → Иерархия групп**
   - **Активы (Устройства) → Задачи**
   - **Мониторинг и отчеты → Отчеты**
   - **Активы (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 пользователю или группе безопасности (см. стр. 430), 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:

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 Linux.

► *Чтобы назначить роль пользователю или группе пользователей, выполните следующие действия:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На вкладке **Права доступа** установите флажок рядом с именем пользователя или группы пользователей, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп пользователей одновременно. Если вы выберете более одного объекта, кнопка **Права доступа** будет неактивна.

3. Настройте набор прав для пользователя или группы:

   a. Разверните узел с функциями Сервера администрирования или другой программы "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции программы**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции программы (**Чтение**, **Запись** и **Выполнение**).

      Пример 2: Разверните узел **Управление ключами шифрования** и установите флажок **Разрешить** рядом с разрешением **Запись**, чтобы предоставить пользователю или группе право доступа на **Запись** к функции управления ключами шифрования.

4. После настройки набора прав доступа нажмите на кнопку **ОК**.

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).
  - Управление ключами шифрования
  - Обработка событий.
  - Операции с Сервером администрирования (только в окне свойств Сервера администрирования).
  - Развертывание программ "Лаборатории Касперского".
  - Управление лицензионными ключами.
  - Интеграция программ
  - Управление отчетами (только для Kaspersky Security Center 11 и выше).
  - Иерархия Серверов администрирования
  - Права пользователя.
  - виртуальные Серверы администрирования;
- Управление мобильными устройствами:
  - Общие
  - Self Service Portal
- Управление системой:
  - Подключения.
  - Инвентаризация оборудования
  - Управление доступом в сеть.
  - Развертывание операционной системы.
  - Системное администрирование.
  - 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 следующего:

- 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.

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 и группы** и выберите вкладку **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Добавить пользователя** укажите параметры нового пользователя:
   - **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. 463).
     Если пользователь неправильно ввел пароль заданное количество раз, учетная запись пользователя блокируется на один час. Вы можете разблокировать учетную запись, только сменив пароль.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новая учетная запись пользователей добавлена в список пользователей.

См. также:

Сценарий: Настройка защиты сети 349

kaspersky

Создание группы безопасности

► *Чтобы создать группу безопасности:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Создать группу безопасности** укажите следующие параметры новой группы безопасности:
   - **Имя группы.**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Новая группа безопасности добавлена в список групп.

См. также:

Сценарий: Настройка защиты сети 349

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 и группы** и выберите вкладку **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 номер телефона.**
   - **Задать новый 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. 463) 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. 451).
7. На закладке **Роли** можно назначить роль пользователю (см. стр. 465).
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей.

См. также:

Сценарий: Настройка защиты сети 349

Изменение группы безопасности

► *Чтобы изменить группу безопасности:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Группы**.
2. Выберите группу безопасности, которую требуется изменить.
3. В открывшемся окне измените параметры группы безопасности:
   - На вкладке **Общие** можно изменить параметры **Имя** и **Описание**. Эти параметры доступны только для внутренних групп безопасности.
   - На вкладке **Пользователи** можно добавить пользователей в группу пользователей (см. стр. 450). Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
   - На вкладке **Роли** можно назначить роль группе безопасности (см. стр. 450).
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

См. также:

Сценарий: Настройка защиты сети 349

Назначение роли пользователю или группе безопасности

► *Чтобы назначить роли пользователю или группе безопасности:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Выберите имя пользователя или группы безопасности, которой нужно назначить роль.

   Можно выбрать несколько имен.
3. В меню нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли.
4. Следуйте инструкциям мастера: выберите роль, которую вы хотите назначить выбранным пользователям или группам безопасности, и выберите область действия роли.

   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.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю (или пользователям или группе безопасности). В списке пользователей или групп пользователей отображается флажок в столбце **Имеет назначенные роли**.

Добавление учетных записей пользователей во внутреннюю группу безопасности

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу безопасности.

► *Чтобы добавить учетные записи пользователей во внутреннюю группу безопасности:*

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи и группы** и выберите вкладку **Пользователи**.
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу безопасности.

3. Нажмите на кнопку **Назначить группу**.
4. В открывшемся окне **Назначить группу** выберите группу безопасности, в которую требуется добавить учетные записи пользователей.
5. Нажмите на кнопку **Сохранить**.

Учетные записи пользователей добавлены в группу безопасности. Также можно добавить внутренних пользователей в группу безопасности, используя параметры группы (см. стр. 449).

См. также:

Сценарий: Настройка защиты сети 349

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 и группы** и выберите вкладку **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 в группе **Активы (Устройства)** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Управление владельцем устройства**.

kaspersky

См. также:

Сценарий: Настройка защиты сети 349

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 и группы** и выберите вкладку **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 **Дополнительные настройки безопасности**.
4. На закладке **Дополнительные настройки безопасности** 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**.

Двухэтапная проверка

В этом разделе описывается использование двухэтапной проверки для снижения риска несанкционированного доступа к Kaspersky Security Center 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 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:

1. Установка приложения проверки подлинности на устройство

   Вы можете установить любое приложение проверки подлинности, которое поддерживает алгоритм формирования одноразового пароля на основе времени (TOTP), такие как:

- Google Authenticator.
- Microsoft Authenticator.
- Bitrix24 OTP.
- Яндекс ключ.
- Avanpost Authenticator.
- Aladdin 2FA.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение проверки подлинности, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением проверки подлинности. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

2. Синхронизация времени приложения проверки подлинности и время устройства, на котором установлен Сервер администрирования

   Убедитесь, что время на устройстве с приложением проверки подлинности и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

3. Включение двухэтапной проверки и получение секретного ключа для своей учетной записи

   После включения двухэтапной проверки для своей учетной записи (см. стр. 457) вы можете включить двухэтапную проверку для всех пользователей.

4. Включение двухэтапной проверки для всех пользователей

   Пользователи с включенной двухэтапной проверкой (см. стр. 458) должны использовать ее для входа на Сервер администрирования.

5. Запретить новым пользователям настраивать для себя двухэтапную проверку

   Чтобы еще больше повысить безопасность доступа к Kaspersky Security Center Web Console, вы можете запретить новым пользователям настраивать для себя двухэтапную проверку (см. стр. 461).

6. Изменение имени издателя кода безопасности

   Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности (см. стр. 462) для лучшего распознавания разных Серверов администрирования.

7. Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку

   При необходимости исключите учетные записи пользователей из двухэтапной проверки (см. стр. 460). Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

8. Настройка двухэтапной проверки для вашей учетной записи

   Если пользователи не исключены из двухэтапной проверки и двухэтапная проверка еще не настроена для их учетных записей, им необходимо настроить ее в окне, открывающемся при входе в Kaspersky Security Center Web Console (см. стр. 460). Иначе они не смогут получить доступ к Серверу администрирования в соответствии со своими правами.

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 учетной записи

Kaspersky Security Center предоставляет двухэтапную проверку для пользователей Kaspersky Security Center Web Console. Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center Web Console вы вводите свое имя пользователя, пароль и 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.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение проверки подлинности, которое вы хотите использовать, включите двухфакторную проверку для всех пользователей или для определенного пользователя.

Один из шагов предполагает, что вы указываете код безопасности, сгенерированный приложением проверки подлинности. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

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 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. 460) 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 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 функциональной области **Общий функционал: Права пользователей** и, который авторизован в Kaspersky Security Center 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 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 и не включаете двухэтапную проверку для учетных записей пользователей подчиненных Серверов администрирования (см. стр. 205).

См. также:

Включение двухэтапной проверки для вашей учетной записи 457

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 и группы** и выберите вкладку **Пользователи**.
2. Нажмите на имя вашей учетной записи.
3. В открывшемся окне свойств пользователя выберите вкладку **Дополнительные настройки безопасности**.
   a. Выберите параметр **Запрашивать только имя пользователя, пароль и код безопасности (двухэтапная проверка). Нажмите на** кнопку **Сохранить.**
   b. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

      Введите секретный ключ в приложении проверки подлинности или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения проверки подлинности на мобильном устройстве, чтобы получить одноразовый код безопасности.
   c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением проверки подлинности и нажмите на кнопку **Проверить и применить**.
4. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи включена.

См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей 453

kaspersky

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 в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

► *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**.

3. Если вы не включили двухэтапную проверку для своей учетной записи, программа откроет окно включения двухэтапной проверки для вашей учетной записи (см. стр. 457).

   a. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

   b. Введите секретный ключ вручную в приложении проверки подлинности или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения проверки подлинности на мобильном устройстве, чтобы получить одноразовый код безопасности.

   c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением проверки подлинности и нажмите на кнопку **Проверить и применить**.

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. 460) из двухэтапной проверки.

См. также:

Сценарий: Настройка двухэтапной проверки для всех пользователей 453

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 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 и группы** и выберите вкладку **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 **Дополнительные настройки безопасности**.
4. 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 453

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 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. 457) 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 453

Исключение учетных записей из двухэтапной проверки.

Вы можете исключить учетные записи пользователей из двухэтапной проверки, если у вас есть право Изменение списков ACL объекта 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. 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 в таблице исключений для двухэтапной проверки нажмите на кнопку **Добавить**.

3. 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 453

Настройка двухэтапной проверки для вашей учетной записи

При первом входе в Kaspersky Security Center после включения двухэтапной проверки открывается окно настройки двухэтапной проверки для вашей учетной записи.

Перед тем как настроить двухэтапную проверку для своей учетной записи, убедитесь, что на вашем мобильном устройстве установлено приложение проверки подлинности. Убедитесь, что время на устройстве с приложением проверки подлинности и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени.

► *Чтобы настроить двухэтапную проверку для учетной записи:*

1. Сгенерируйте одноразовый код безопасности с помощью приложения проверки подлинности на мобильном устройстве. Для этого выполните одно из следующих действий:
   - Введите секретный ключ в приложение проверки подлинности вручную.
   - Нажмите на кнопку **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения проверки подлинности.

   Код безопасности отобразится на вашем мобильном устройстве.
2. В окне Настройка двухэтапной проверки укажите код безопасности, сгенерированный приложением проверки подлинности и нажмите на кнопку **Проверить и применить**.

Двухэтапная проверка для вашей учетной записи настроена. У вас есть доступ к Серверу администрирования в соответствии со своими правами.

Запретить новым пользователям настраивать для себя двухэтапную проверку

Чтобы еще больше повысить безопасность доступа к Kaspersky Security Center Web Console, вы можете запретить новым пользователям настраивать для себя двухэтапную проверку.

Если этот параметр включен, пользователь с выключенной двухэтапной проверкой, например новый администратор домена, не сможет настроить двухэтапную проверку для себя. Следовательно, такой пользователь не может быть аутентифицирован на Сервере администрирования и не может войти в Web Console без одобрения другого администратора Kaspersky Security Center, у которого уже включена двухэтапная проверка.

Этот параметр доступен, если для всех пользователей включена двухэтапная проверка (см. стр. 458).

► *Чтобы запретить новым пользователям настраивать для себя двухэтапную проверку:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Дополнительные настройки безопасности** в окне свойств включите переключатель **Запретить новым пользователям настраивать двухэтапную аутентификацию для себя.**

Этот параметр не влияет на учетные записи пользователей, добавленных в исключения двухэтапной проверки (см. стр. 460).

Чтобы предоставить доступ к Kaspersky Security Center Web Console пользователю с выключенной двухэтапной проверкой, временно выключите параметр **Запретить новым пользователям настраивать**

двухэтапную проверку для себя, попросите пользователя включить двухэтапную проверку, а затем включите параметр снова.

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 и группы** и выберите вкладку **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 **Дополнительные настройки безопасности**.
4. На вкладке **Дополнительные настройки безопасности** 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 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 **Дополнительные настройки безопасности**.

3. На вкладке **Дополнительные настройки безопасности**, перейдите по ссылке **Редактировать**.

   Откроется раздел **Изменить код безопасности издателя**.

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 453

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, выполните следующие действия:*

1. На Сервере администрирования запустите командную строку Linux
2. Для утилиты klscflag выполните следующую команду:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   где N – количество попыток ввода пароля.

3. Чтобы изменения вступили в силу, перезапустите службу Сервера администрирования.

Максимальное количество попыток ввода пароля изменено.

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 и группы** и выберите вкладку **Пользователи** или **Группы**.
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 349

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. 465).
   - 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 349

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, а также политики и профили политик, связанные с ролью (см. стр. 465).
- 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 349

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 и группы** и выберите вкладку **Пользователи** или **Группы**.
2. Установите флажки напротив имен пользователей или 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 безопасности, которые требуется добавить в область роли.
7. Нажмите на кнопку **Назначить роль**, чтобы закрыть окно мастера.
8. Нажмите на кнопку **Закрыть** (✕), чтобы закрыть окно свойств.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

См. также:

Сценарий: Настройка защиты сети 349

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 **ОК**.

Роль пользователя будет удалена.

См. также:

Сценарий: Настройка защиты сети 349

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. 430) 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 вкладку **Параметры** и прокрутите 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 **Новый профиль политики**.
     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 роли**.

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 349

kaspersky

Обновление баз и программ "Лаборатории Касперского"

Установка обновлений исполняемых модулей программ "Лаборатории Касперского", не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программы из сертифицированного 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. 349), 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, программ "Лаборатории Касперского" и программных модулей вручную (см. стр. 492) 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 Web Console (см. стр. 299).
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. стр. 349).
3. Назначено соответствующее количество точек распространения (см. стр. 204) в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и программ "Лаборатории Касперского" состоит из следующих этапов:

1. Выбор схемы обновления

   Существует несколько схем (см. стр. 471), 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.

e. 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.

Инструкция: Создание задачи для загрузки обновлений в хранилище Сервера администрирования (см. стр. 477).

f. 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.

Инструкция: Создание задачи загрузки обновлений в хранилища точек распространения (см. стр. 484).

g. Настройка точек распространения

Если в вашей сети назначены точки распространения, 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.

h. Оптимизация процесса обновления с помощью файлов различий (если требуется)

Вы можете оптимизировать трафик между Сервером администрирования и управляемыми устройствами с помощью файлов различий (см. стр. 490). 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 или точками распространения 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*.

Инструкция: Использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского" (см. стр. 490)

i. Настройка автоматической установки обновлений для программ безопасности

Создайте задачу *Обновление* для управляемых программ, чтобы обеспечить своевременное обновление 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. 410).

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 и Агент администрирования версии 13.2.

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.

Результаты

После завершения сценария, Kaspersky Security Center настроен на обновление баз "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования. Теперь вы можете приступить к мониторингу состояния сети.

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. 171). Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

  Kaspersky Security Center не может обновлять программы "Лаборатории Касперского" автоматически. Чтобы обновить программы, загрузите последние версии программ с сайта "Лаборатории Касперского" и установите их вручную:

  - Сервер администрирования Kaspersky Security Center, Kaspersky Security Center Web Console https://www.kaspersky.ru/small-to-medium-business-security/downloads/security-center
  - Агент администрирования, Kaspersky Endpoint Security, веб-плагин управления https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint

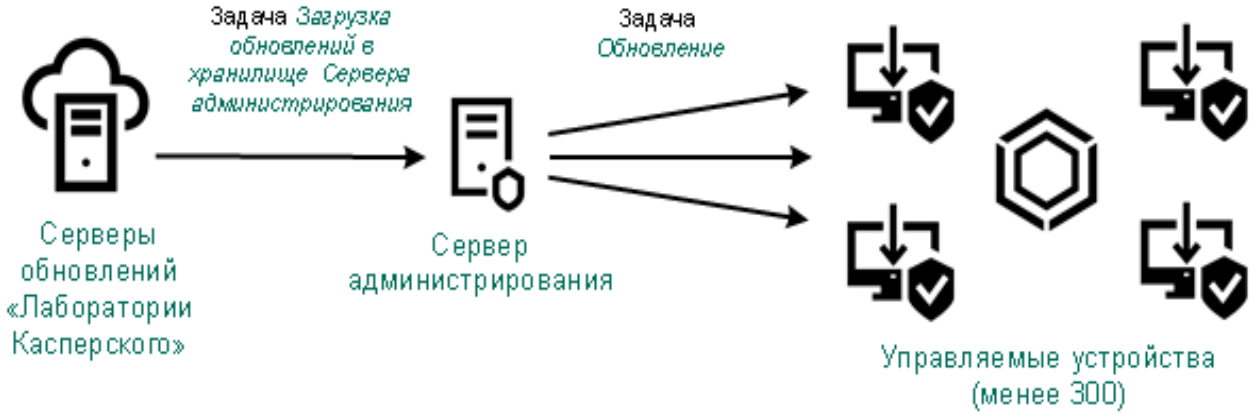
В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- С помощью одной задачи: *Загрузка обновлений в хранилище Сервера администрирования*
- С помощью двух задач:
  - *Задачи* Загрузка обновлений в хранилище Сервера администрирования.
  - *Задачи* Загрузка обновлений 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 *Загрузка обновлений 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).



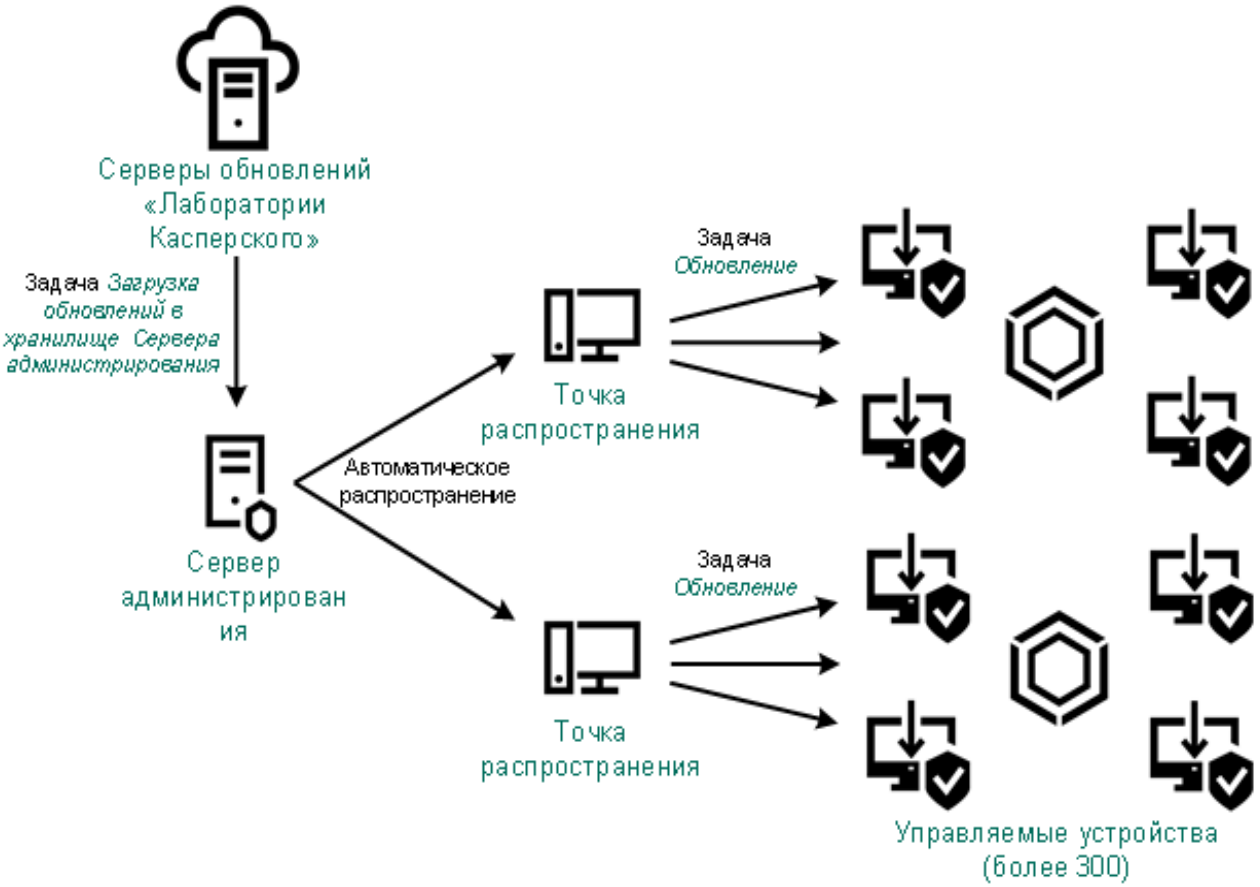
В качестве источника обновлений (см. стр. 489) можно использовать не только серверы обновлений "Лаборатории Касперского", но и локальную или сетевую папку.

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. 202) 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. 204) 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 выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*, обновления баз "Лаборатории Касперского" и программные модули для Kaspersky Endpoint Security загружены в хранилище Сервера администрирования. Эти обновления устанавливаются с помощью задачи *Обновление* Kaspersky Endpoint Security.

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.

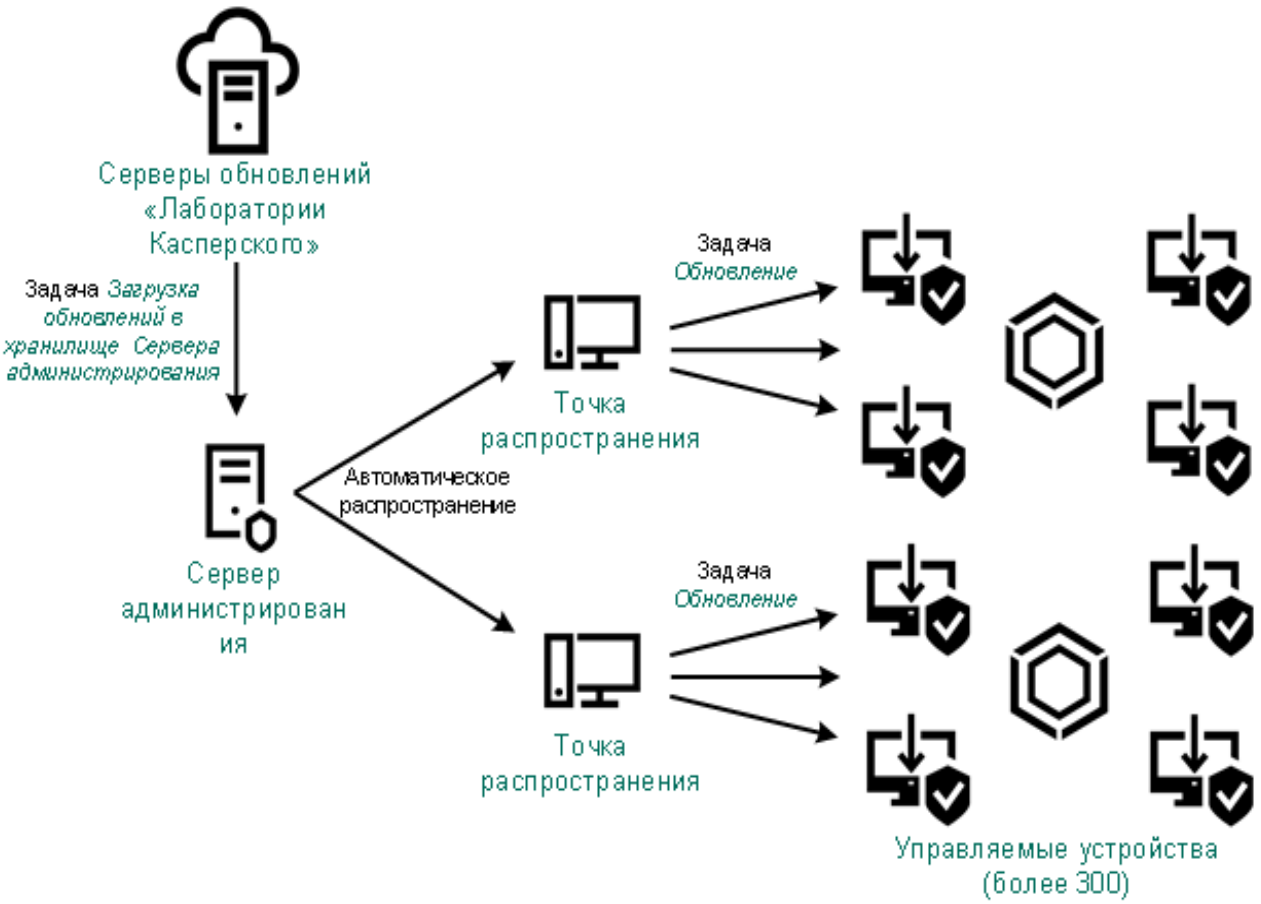
Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются программами. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений 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.



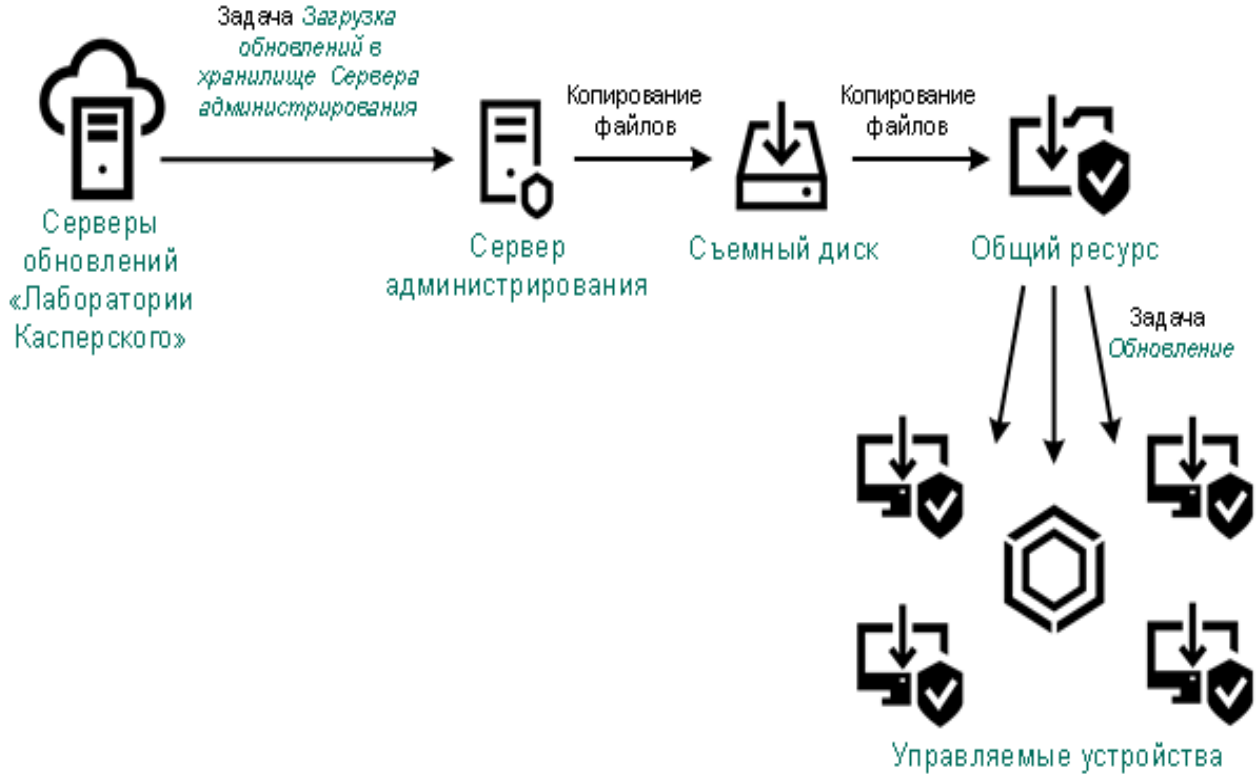
По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Для этой схемы также требуется задача *Загрузка обновлений 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. 492). 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 параметрах Kaspersky Endpoint Security (см. рисунок ниже).

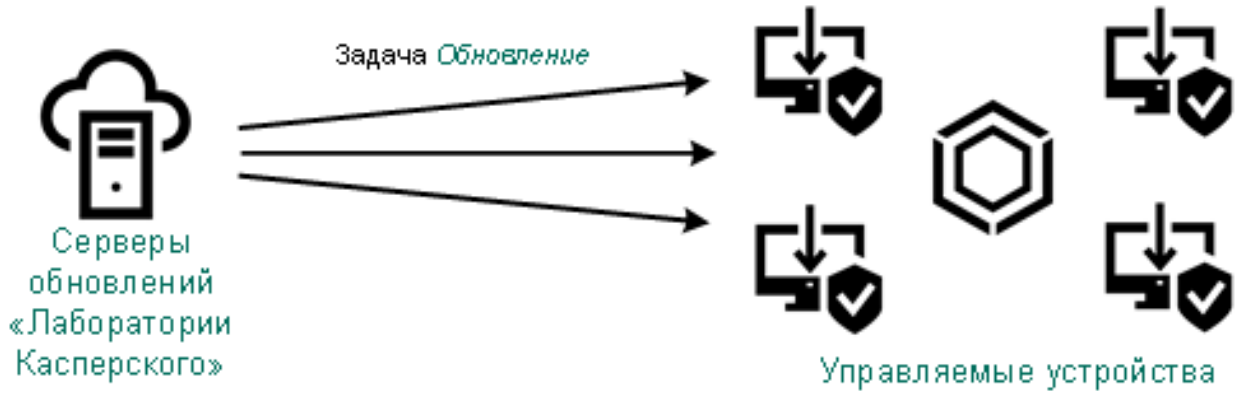


Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Онлайн-справка Kaspersky Endpoint Security для Linux
- Онлайн-справка Kaspersky Endpoint Security для Windows

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 программа безопасности не использует хранилище, предоставленное Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в программе безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Онлайн-справка Kaspersky Endpoint Security для Linux
- Онлайн-справка Kaspersky Endpoint Security для Windows

Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

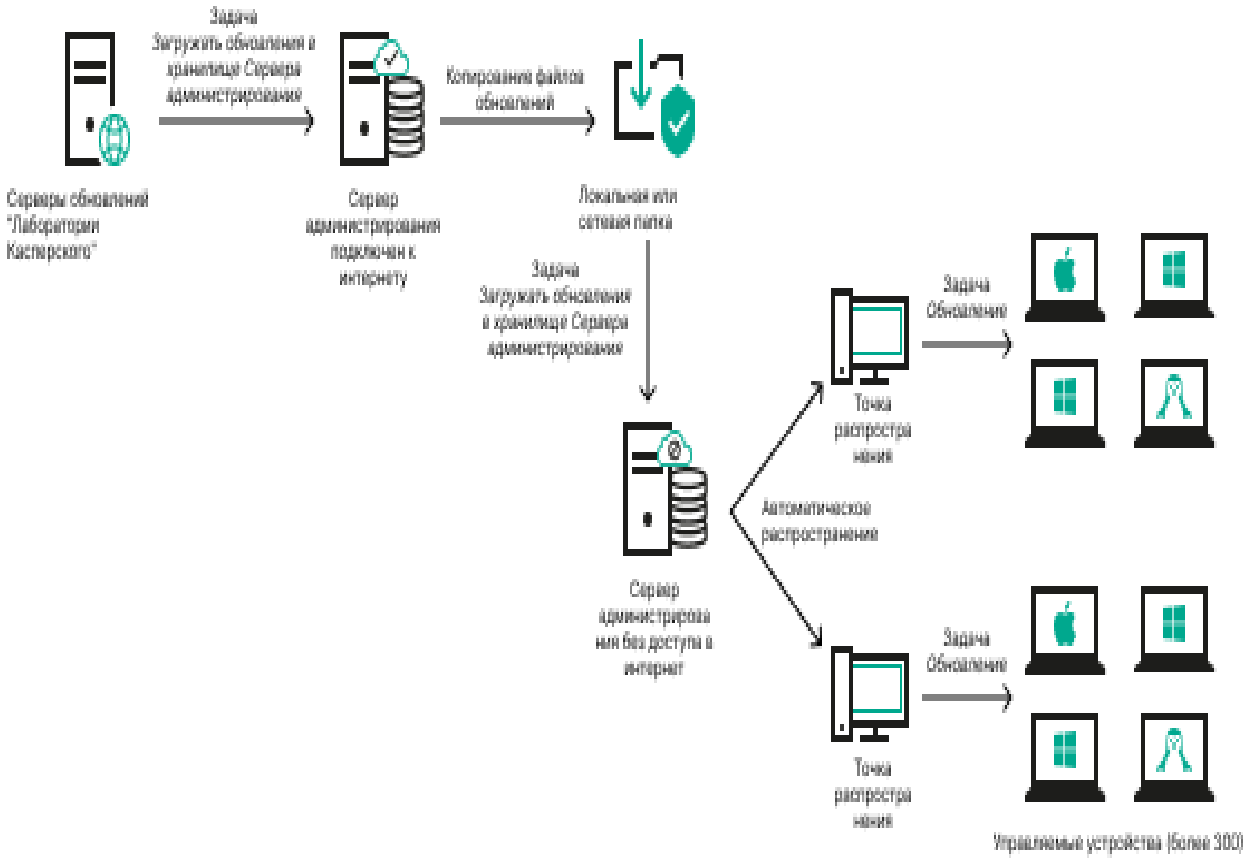
Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. 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, а затем включите параметр **Загружать обновления, используя старую схему** (см. стр. 477).



- Kaspersky Update Utility https://support.kaspersky.com/updater4

  Так как утилита использует старую схему для загрузки обновлений, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр *Загружать обновления, используя старую схему* (см. стр. 477).

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и программных модулей программы безопасности "Лаборатории Касперского" с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования.

Мастер первоначальной настройки Kaspersky Security Center автоматически создает задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 135). В списке

задач может быть только одна задача *Загрузка обновлений в хранилище Сервера администрирования*. Вы можете создать эту задачу повторно, если она будет удалена из списка задач Сервера администрирования.

После завершения задачи *Загрузка обновлений в хранилище Сервера администрирования* и загрузки обновлений их можно распространять на управляемые устройства.

Перед распространением обновлений на управляемые устройства вы можете выполнить задачу *Проверка обновлений* (см. стр. 482). 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 **Выполнять проверку обновлений перед распространением** в параметрах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

► *Чтобы создать задачу загрузки обновлений в хранилище Сервера администрирования, выполните следующие действия:*

1. В главном окне программы перейдите к закладке **Активы (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. 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. Также можно настроить параметры задачи позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.
7. Чтобы открыть окно свойств задачи, нажмите на имя созданной задачи.
8. В окне свойств задачи на закладке **Параметры программы** укажите следующие параметры:
   - **Источники обновлений**

В качестве источника обновлений можно использовать серверы обновлений "Лаборатории Касперского", локальную или сетевую папку или главный Сервер администрирования (см. стр. 489).

В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала создайте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Kaspersky Security Center не потребует от вас ввода учетных данных.

   - **Папка для хранения обновлений**

- **Форсировать обновление подчиненных Серверов администрирования**

  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.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий (см. стр. 490).

  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 проверки обновлений, указанную в поле **Задача проверки обновлений** (см. стр. 482). 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**:
     - **Вручную** (выбрано по умолчанию)

       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.

- **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.

- Дополнительные параметры задачи:
  - **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.

1. Нажмите на кнопку **Сохранить**.

Задача создана и настроена.

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 Сервера администрирования. 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:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Просмотр полученных обновлений

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 Сервера администрирования. Вы можете просмотреть загруженные обновления в разделе **Обновления баз и программных модулей "Лаборатории Касперского"**.

► *Чтобы просмотреть список полученных обновлений,*

В главном окне программы перейдите в раздел **Операции** → **Программы "Лаборатории Касперского"** → **Обновления баз и программных модулей "Лаборатории Касперского"**.

Отобразится список доступных обновлений.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Создание задачи Загрузка обновлений в хранилище Сервера администрирования 477

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 *Загрузка обновлений 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 с несколькими тестовыми устройствами (см. стр. 243). 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 для какой-нибудь программы, которую поддерживает Kaspersky Security Center, например, Kaspersky Endpoint Security для Linux (см .стр. 408). 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. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 477).

► *Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на вкладку **Параметры программы** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **Выберите задачу**. В открывшемся окне выберите задачу *Проверка обновлений* в группе администрирования с тестовыми устройствами.

5. Если вы не создавали задачу *Проверка обновлений* ранее, выполните следующие действия:
   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 **Указать учетную запись** и введите учетные данные этой учетной записи.
6. Закройте окно **свойств задачи** *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку *Сохранить*.

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".....468

Создание задачи загрузки обновлений в хранилища точек распространения

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 безопасности "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, выполните следующие действия:*

1. В главном окне программы перейдите к закладке **Активы (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 хранилища 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 **Создать**.

   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 проверки подлинности, 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".

В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала создайте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Kaspersky Security Center не потребует от вас ввода учетных данных.

- **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. 490).

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

1. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию**:
  - **Вручную** (выбрано по умолчанию)

    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.

- **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:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования

При создании или использовании задачи загрузки обновлений в хранилище Сервера администрирования (см. стр. 471), вы можете выбрать следующие источники обновлений:

- Серверы обновлений "Лаборатории Касперского"
- Главный Сервер администрирования

  Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
- Локальная или сетевая папка

  В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала создайте защищенную паролем папку, а затем укажите необходимые учетные данные, например, средствами операционной системы. После этого вы можете выбрать эту папку в качестве источника обновлений в задаче загрузки обновлений. Kaspersky Security Center не потребует от вас ввода учетных данных.

Серверы обновлений "Лаборатории Касперского" используются по умолчанию, но можно также загружать обновления из локальной или сетевой папки. Вы можете использовать эту папку, если ваша сеть не имеет доступа к интернету. В этом случае можно вручную загрузить обновления с серверов обновлений "Лаборатории Касперского" и поместить загруженные файлы в нужную папку.

Вы можете указать только один путь к локальной или сетевой папке. В качестве локальной папки необходимо указать папку на устройстве, где установлен Сервер администрирования В качестве сетевой папки можно использовать FTP-сервер или HTTP-сервер или общий ресурс SMB. Если общий ресурс SMB требует аутентификации, его необходимо заранее подключить к системе с необходимыми учетными данными. Не рекомендуется использовать протокол SMB1, так как он небезопасен.

Если вы добавите и серверы обновлений "Лаборатории Касперского", и локальную или сетевую папку, то сначала будут загружаться обновления из папки. В случае ошибки при загрузке будут использоваться серверы 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.

► *Чтобы добавить источники обновлений:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.

2. Нажмите на **Загрузка обновлений в хранилище Сервера администрирования**.
3. Перейдите на закладку **Параметры программы**.
4. Около **Источники обновлений** нажмите на кнопку **Настроить**.
5. В появившемся окне нажмите на кнопку **Добавить**.
6. В списке источников обновлений добавьте необходимые источники. Если вы установите флажок **Локальная или сетевая папка**, укажите путь к папке.
7. Нажмите на кнопку **ОК**, а затем закройте окно свойств источника обновлений.
8. В окне источника обновлений нажмите на кнопку **ОК**.
9. Нажмите на кнопку **Сохранить** в окне задач.

Обновления загружаются в хранилище Сервера администрирования из указанных источников.

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.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Включение функции загрузки файлов различий: сценарий.....491

Включение функции загрузки файлов различий: сценарий

Этапы

1. Включение функции на Сервере администрирования

   Включите функцию в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 477).

2. Включение функции для точки распространения

   Включить функцию для точки распространения, которая получает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения* (см. стр. 484).

   Включите функцию в параметрах политики Агента администрирования для точки распространения, которая получает обновления с Сервера администрирования (см. стр. 382).

   Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

   Эта функция включается в свойствах политики Агента администрирования (см. стр. 382) и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения** (см. стр. 491).

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".....490

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Об обновлении баз, программных модулей и программ "Лаборатории Касперского".....471

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, выполните следующие действия:*

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, через которую будут доставляться обновления на клиентские устройства в группе.
4. В окне свойств точки распространения выберите раздел **Источник обновлений**.
5. Выберите источник обновлений для точки распространения:
   - **Источник обновлений**
   - **Загрузить файлы различий**

Этот параметр включает функцию загрузки файлов различий (см. стр. 490).

По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

См. также:

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского".....468

Обновление баз и программных модулей "Лаборатории Касперского" на автономных устройствах

Установка обновлений исполняемых модулей программ "Лаборатории Касперского", не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу программы из сертифицированного состояния.

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. 468) с помощью хранилища Сервера администрирования.

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 *Download updates to the Administration Server repository*.

- 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 *Загрузка 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 Kaspersky Endpoint Security на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.

   Инструкции:

   - Онлайн-справка Kaspersky Endpoint Security для Linux
   - Онлайн-справка Kaspersky Endpoint Security для Windows
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, требующем установки обновлений, запустите задачу Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows *Обновление*, в зависимости от операционной системы автономного устройства.

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".....468

Создание задачи Загрузка обновлений в хранилище Сервера администрирования 477

kaspersky

Резервное копирование и восстановление веб-плагинов

Kaspersky Security Center 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** → **Веб-плагины**.
2. В разделе **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 вкладке **Резервные копии данных**.

► *Чтобы восстановить веб-плагин из резервной копии данных:*

1. В главном окне программы перейдите в раздел **Параметры** → **Резервные копии данных**.
2. В разделе **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.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В программе Kaspersky Security Center, находящемся в открытом сегменте сети, настроить задачу загрузки обновлений в хранилище.
2. Убедиться в том, что под управлением Kaspersky Security Center в открытом сегменте есть управляемые машины с установленными программами, базы для которых необходимо обновить.
3. Запустить задачу. В процессе загрузки обновлений с открытых серверов "Лаборатории Касперского" Kaspersky Security Center проведет проверку контроля целостности обновлений, прежде чем добавит их в свое хранилище.
4. Удобным вам способом перенесите содержимое хранилища Kaspersky Security Center в изолированный сегмент сети.

Запустите на средствах антивирусной защиты внутри изолированного сегмента сети задачу обновления с указанием перенесенного хранилища как источника обновлений. При загрузке обновлений из хранилища, средства антивирусной защиты еще раз проведут контроль целостности загружаемых обновлений.

kaspersky

Мониторинг, отчеты и аудит

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:

1. **Настройка переключения статусов устройств**

   Ознакомьтесь с параметрами статусов устройства в зависимости от конкретных условий. Изменяя эти параметры (см. стр. 551), 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.

j. 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. 552).

k. Выполнение рекомендуемых действий для критических и предупреждающих уведомлений

Инструкции:

Выполните рекомендуемые действия для сети вашей организации (см. стр. 546).

l. Просмотр состояния безопасности сети вашей организации

Инструкции:

Просмотр веб-виджета Состояние защиты (см. стр. 499).

Генерация и просмотр отчета о состоянии защиты (см. стр. 510).

Генерация и просмотр отчета об ошибках (см. стр. 510).

m. Нахождение незащищенных клиентских устройств

Инструкции:

Просмотр веб-виджета Новые устройства (см. стр. 499)

Генерация и просмотр отчета о развертывании защиты (см. стр. 510).

n. Проверка защиты клиентских устройств

Инструкции:

Генерация и просмотр отчета из категорий Статус защиты и Статистика угроз (см. стр. 510).

Запуск и просмотр выборки событий Критические (см. стр. 537).

o. 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:

Ограничение максимального количества событий (см. стр. 165).

p. Просмотр информации о лицензии

Инструкции:

Добавление веб-виджета Используемые лицензионные ключи на панель мониторинга и его просмотр (см. стр. 499).

Генерация и просмотр отчета Отчет об использовании лицензионных ключей (см. стр. 510).

Результаты

После завершения сценария вы будете проинформированы о защите сети вашей организации и, таким образом, сможете планировать действия для дальнейшей защиты.

О типах мониторинга и отчетах

Информация о событиях безопасности в сети организации хранится в базе данных Сервера администрирования. Kaspersky Security Center 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 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 мониторинга 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 Web Console в разделе **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 Web Console имеет по умолчанию набор веб-виджетов для следующих категорий:

- **Состояние защиты**
- **Развертывание.**
- **Обновления.**
- **Статистика угроз**
- **Другое**

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. 500), скрывать веб-виджеты (см. стр. 500), а также менять внешний вид или размер веб-виджетов (см. стр. 501), перемещать веб-виджеты (см. стр. 501) и изменять параметры веб-виджетов (см. стр. 502).

См. также:

Сценарий: Мониторинг и отчеты 496

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 или восстановить 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. 501) и параметры (см. стр. 502) добавленных веб-виджетов.

См. также:

Сценарий: Мониторинг и отчеты 496

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 пункт **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. 500).

kaspersky

См. также:

Сценарий: Мониторинг и отчеты 496

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 пункт **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 496

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 столбчатая диаграмма)**
     - **Средний (кольцевой график)**

- **Средний (столбчатая диаграмма)**
- **Средний**

Внешний вид выбранного веб-виджета будет изменен.

См. также:

Сценарий: Мониторинг и отчеты 496

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 496

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга (см. стр. 503) 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. 432) в функциональной области **Общие функции: Права пользователя**.

См. также:

Настройка режима Просмотра только панели мониторинга.....503

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга (см. стр. 502) убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменения списков управления доступом к объектам** (см. стр. 432) 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. 432) в области **Общий функционал: 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 на вкладке **Пользователи** в разделе **Пользователи и роли → Пользователи и группы**. 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 и группы** и выберите вкладку **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 вкладке **Панель мониторинга** можно выполнять те же действия с веб-виджетами, что и в разделе **Мониторинг и отчеты** → **Панель мониторинга**:

   - Добавлять веб-виджеты (см. стр. 500) на панель мониторинга.
   - Скрывать веб-виджеты (см. стр. 500), которые не нужны пользователю.
   - Перемещать веб-виджеты (см. стр. 501) в определенном порядке.
   - Изменять размер или внешний вид (см. стр. 501) веб-виджетов.
   - Изменение параметров веб-виджетов (см. стр. 502).

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. 432) 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.

kaspersky

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 Web Console в разделе **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.**
- **Обновления.**
- **Статистика угроз**
- **Другое**

Вы можете создавать пользовательские шаблоны отчетов (см. стр. 505), редактировать шаблоны отчетов (см. стр. 506) и удалять их (см. стр. 511).

Можно создавать отчеты (см. стр. 510) на основе существующих шаблонов, экспортировать отчеты в файл (см. стр. 509) и создавать задачи рассылки отчетов (см. стр. 510).

См. также:

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 **OK**, 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 496

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. 510), а затем нажать на кнопку **Изменить**.
3. Нажмите на кнопку Открыть свойства шаблона отчета**.**

   Откроется окно **Изменение отчета <Имя отчета>** на вкладке **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. Обратите внимание, что этот параметр не влияет на максимальное количество событий, которые вы можете включить в отчет при экспорте отчета в файл (см. стр. 509).

    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.
  - **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.

- **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 сохранить один или несколько отчетов в форматах XML, HTML или PDF. Kaspersky Security Center позволяет экспортировать до 10 отчетов в файлы указанного формата одновременно.

► *Чтобы экспортировать отчет в файл:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Выберите отчеты, которые вы хотите экспортировать.

   Если вы выберете более десяти отчетов, кнопка **Экспортировать отчет** будет неактивна.
3. Нажмите на кнопку **Экспортировать отчет**.
4. В открывшемся окне настройте следующие параметры экспорта:
   - **Имя файла**.

     Если вы выбрали один отчет для экспорта, укажите имя файла отчета.

     Если вы выбрали несколько отчетов, имена файлов отчетов будут совпадать с именами выбранных шаблонов отчетов.
   - **Максимальное количество записей**.

     Укажите максимальное количество записей, которые будут включены в файл отчета. По умолчанию указано значение 10,000.

     Вы можете экспортировать отчет с неограниченным количеством записей. Обратите внимание, что если ваш отчет содержит большое количество записей, время, необходимое для создания и экспорта отчета, увеличивается.
   - **Формат файла**.

     Выберите формат файла отчета: XML, HTML или PDF. При экспорте нескольких отчетов все выбранные отчеты сохраняются в указанном формате в виде отдельных файлов.

Утилита wkhtmltopdf необходима для преобразования отчета в формат PDF. При выборе параметра PDF, Сервер администрирования проверяет установлена ли на устройстве утилита wkhtmltopdf. Если утилита не установлена, программа выводит сообщение о необходимости установки утилиты на устройство Сервера администрирования. Установите утилиту вручную, а затем перейдите к следующему шагу.

5. Нажмите на кнопку **Экспортировать отчет**.

Отчет будет сохранен в файл в указанном формате.

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 сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

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: Мониторинг и отчеты 496

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.

      Утилита wkhtmltopdf необходима для преобразования отчета в формат PDF. При выборе параметра PDF, Сервер администрирования проверяет установлена ли на устройстве утилита wkhtmltopdf. Если утилита не установлена, программа выводит сообщение о необходимости установки утилиты на устройство Сервера администрирования. Установите утилиту вручную, а затем перейдите к следующему шагу.
   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.

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:

Сценарий: Мониторинг и отчеты 496

kaspersky

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 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.

События по типу

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 по источнику

Просмотреть полный список событий, которые может генерировать программа, можно на вкладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими программами:

- Компоненты программы Kaspersky Security Center:
  - Сервер администрирования (см. стр. 514)
  - Агент администрирования (см. стр. 533)
- Управляемые программы "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми программами "Лаборатории Касперского", см. в документации соответствующей программы.

События по уровню важности

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 компонент Kaspersky Security Center 513

Сценарий: Настройка экспорта событий в SIEM-системы 562

События компонент 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 и Агенте администрирования. 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 вкладке **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 в свойствах Сервера администрирования (см. стр. 552).

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: Настройка срока хранения события (см. стр. 541).

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

kaspersky

В этом разделе

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на вкладке **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 в свойствах Сервера администрирования (см. стр. 552).

Таблица 38. 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. 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. 332), охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий (см. стр. 345) при превышении лицензионного ограничения.	180 дней
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. Определите, что мешает правильной работе Агента администрирования на устройстве. Возможные причины могут включать проблемы сети и удаление Агента администрирования с устройства.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Статус устройства "Критический".	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия (на стр. 267) при выполнении которых, статус устройства изменяется на *Критический*.	180 дней
Файл ключа добавлен в список запрещенных.	4124	KLSRV_LICENSE_BLACKLISTED	События этого типа возникают, если "Лаборатория Касперского" добавила код активации или лицензионный ключ, который вы используете, в запрещенный список. Обратитесь в Службу технической поддержки для получения подробной информации.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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. 331). 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. Это количество дней нельзя изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center работает в режиме Базовой функциональности (см. стр. 333). Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ (см. стр. 332) добавлен на Сервер администрирования. • Если вы используете подписку, продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Срок действия сертификата истек.	4132	KLSRV_CERTIFICATE_EXPIRED	События этого типа возникают, если истекает срок действия сертификата Сервера администрирования для Управления мобильными устройствами. Вам необходимо обновить сертификат, срок действия которого истекает. Вы можете настроить автоматическое обновление сертификатов, установив флажок **Автоматически перевыпускать сертификат, если это возможно** в параметрах выпуска сертификата.	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 вкладке **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 в свойствах Сервера администрирования (см. стр. 552).

Таблица 39. 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. Чаще всего это проблемы СУБД, проблемы с сетью и другие проблемы с программным и аппаратным обеспечением. 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 лицензионными ключами программ сторонних производителей и если количество установок превысило заданное в лицензионном ключе программы стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите программу стороннего производителя с устройств, на которых она не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами программ сторонних производителей, используя функциональность групп лицензионных программ. В группу лицензионных программ входят программы сторонних производителей, отвечающие заданным вами критериям.	180 дней
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). Вы можете ответить на событие следующими способами: • Проверьте, имеет ли учетная запись пользователя, которая используется для получения доступа к папке (или папкам), права на запись. • Проверьте, не были ли изменены имя пользователя и/или пароль к папке (к папкам). • Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и программных модулей.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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. 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 недоступна (стр. 124). Вы можете ответить на событие следующими способами: • Убедитесь, что Сервер администрирования (на котором находится общая папка) включен и доступен. • Проверьте, были ли изменены имя пользователя и/или пароль к папке. • Проверьте подключение к сети.	180 дней
База данных Сервера администрирования недоступна.	4109	KLSRV_DATABASE_UNAVAILABLE	События этого типа возникают, если база Сервера администрирования становится недоступной. Вы можете ответить на событие следующими способами: • Проверьте, доступен ли удаленный сервер, на котором установлен SQL-сервер. • 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.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию

Нет свободного места в базе Сервера администрирования.	4110	KLSRV_DATABASE_FULL	События этого типа возникают, если нет свободного места в базе Сервера администрирования.
			Сервер администрирования не работает, если его база данных переполнена и дальнейшая запись в базу данных невозможна.
			Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие:
			• Вы используете SQL Server Express Edition:
			  • 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. 165).
			  • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.
			• Вы используете СУБД, отличную от SQL Server Express Edition:
			  • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 165).
			  • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 541).
			Просмотрите информацию о выборе СУБД (см. стр. 199).
				180 дней

kaspersky

См. также:

События предупреждения Сервера администрирования

В таблице ниже 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 вкладке **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 в свойствах Сервера администрирования (см. стр. 552).

Таблица 40. 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 управляемом устройстве. Дополнительную информацию см. в следующих разделах: Блокировка частых событий (см. стр. 542).	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Лицензионное ограничение превышено.	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. 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. 332) одной лицензии составляет от 100% до 110% от общего количества единиц, охватываемых лицензией. Даже если возникает это событие, клиентские устройства защищены. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите устройства, которые не используются. • Предоставьте лицензию на большее количество устройств (добавьте еще один действительный код активации или файл ключа на Сервер администрирования). Kaspersky Security Center определяет правила генерации событий (см. стр. 345) при превышении лицензионного ограничения.	90 дней
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. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Kaspersky Security Center Web Console (см. стр. 297). • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Kaspersky Security Center Web Console (см. стр. 297).	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Конфликт имен устройств.	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. 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. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве (см. стр. 213).	90 дней
Статус устройства "Предупреждение".	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия (см. стр. 267) 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, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если программа стороннего производителя не используется на каких-то управляемых устройствах, удалите программу с этих устройств. • 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. Вы можете управлять лицензионными ключами программ сторонних производителей, 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. Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие: • 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. • 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. После удаления сертификата мобильные устройства, подключенные по этому сертификату, не смогут подключиться к Серверу администрирования. 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. 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. При истечении срока действия APNs-сертификата, вам необходимо вручную обновить APNs-сертификат и установить его на Сервер iOS MDM. Рекомендуется запланировать обновление APNs-сертификата до истечения срока его действия.	Не хранится

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-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. 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 FCM сообщения на FCM 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). Ниже приведены возможные причины событий и соответствующие реакции в ответ на событие: • 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"). • Проблемы на стороне прокси-сервера (если вы используете прокси-сервер). Прочтите HTTP код в описании события и ответьте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Не удалось отправить FCM-сообщение на FCM 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. Прочтите информацию в описании события и отреагируйте соответствующим образом. 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. Освободите дисковое пространство на устройстве.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Мало свободного места в 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. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • 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. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 165). • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 165). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 541). Просмотрите информацию о выборе СУБД (см. стр. 199).	90 дней
Разорвано соединение с подчиненным Сервером администрирования.	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с подчиненным Сервером администрирования. Прочтите журнал событий Kaspersky Event Log на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Разорвано соединение с главным Сервером администрирования.	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. 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. Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console.	90 дней
Превышено ограничение числа событий, началось удаление событий из базы данных.	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. 544). Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования (на стр. 165). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 541).	Не хранится
Превышено ограничение числа событий, удалены события из базы данных.	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. 544). Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования (см. стр. 165). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 541).	Не хранится

kaspersky

См. также:

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Информационное**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на вкладке **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 в свойствах Сервера администрирования (см. стр. 552).

Таблица 41. Информационные события Сервера администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Лицензионный 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	
Идентификатор экземпляра FCM 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: Подключение к Серверу администрирования.	4147	KLAUD_EV_SERVERCONNECT	30 дней	
Аудит: Изменение объекта.	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • Группа администрирования • группах безопасности; • Пользователь • инсталляционных пакетах; • Задача • Политика • Серверах; • 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: 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: • Пользователь • Лицензия • Сервер; • виртуальный Сервер.
Аудит: Изменение параметров разрешений.	4153	KLAUD_EV_OBJECTACLMODIFIED	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
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 предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования (см. стр. 552).

Таблица 42. События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Произошла проблема безопасности.	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

kaspersky

См. также:

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center с уровнем важности **Информационное сообщение**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики программы. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования (см. стр. 552).

Таблица 43. Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
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
Удалена наблюдаемая программа.	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено.	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено.	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Найдено новое устройство.	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано.	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию

См. также:

События предупреждения Агента администрирования 533

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 Web Console.

Выборки событий доступны в Kaspersky Security Center Web Console в разделе **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. 531).

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий (см. стр. 536). 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. 536).
- Сгенерируйте выборку событий (см. стр. 537).
- Просмотрите сведения о выбранных выборках событий (см. стр. 539).
- Удалите выборку событий (см. стр. 541).
- Удалять события из базы данных Сервера администрирования (см. стр. 540).

См. также:

Выборки устройств.....272

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 результату выборки**.
6. Нажмите на кнопку **Сохранить**, чтобы подтвердить создание выборки событий.

Если был установлен флажок **Перейти к результату выборки**, результат выборки событий будет отображен на экране. В противном случае новая выборка событий появится в списке выборок событий.

См. также:

Сценарий: Мониторинг и отчеты 496

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 496

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 496

kaspersky

Экспорт выборки событий

Kaspersky Security Center позволяет сохранить выборку событий и ее параметры в файл KLO. Вы можете использовать файл KLO для импорта сохраненной выборки событий как в Kaspersky Security Center Windows, так и в Kaspersky Security Center (см. стр. 538).

Обратите внимание, что можно удалять только определенные пользователем выборки событий. Набор выборок событий, заданных по умолчанию в Kaspersky Security Center (предопределенные выборки), не может быть сохранен в файл.

► *Чтобы экспортировать выборку событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется экспортировать.

   Невозможно экспортировать несколько выборок событий одновременно. Если вы выберете более одной выборки, кнопка **Экспортировать** будет неактивна.
3. Нажмите на кнопку **Экспорт**.
4. В открывшемся окне **Сохранить как** укажите имя и путь к файлу выборки событий, а затем 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 выборки событий автоматически сохраняется в папку **Загрузки**.

Импорт выборки событий

Kaspersky Security Center позволяет импортировать выборку событий из файла KLO. Файл KLO содержит экспортированную выборку событий и ее параметры (см. стр. 538).

► *Чтобы импортировать выборку событий:*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Нажмите на кнопку **Импортировать**, чтобы выбрать файл выборки событий, который вы хотите импортировать.
3. В открывшемся окне укажите путь к файлу KLO и нажмите на кнопку **Открыть**. Обратите внимание, что вы можете выбрать только один файл выборки событий.

   Начнется обработка выборки событий.

Появится уведомление с результатами импорта. Если выборка событий импортирована, вы можете перейти по ссылке **Просмотреть сведения об импорте**, чтобы просмотреть свойства выборки.

После успешного импорта выборка событий отображается в списке выборок. Также импортируются параметры выборки событий.

Если имя новой импортированной выборки событий идентично имени существующей выборки, имя импортированной выборки расширяется с помощью окончания вида **(<порядковый номер>)**, например: **(1)**, **(2)**.

Просмотр информации о событии

► *Чтобы просмотреть детальную информацию о событии:*

1. Запустите выборку событий (см. стр. 537).
2. Нажмите на требуемое событие.

   Откроется окно **Свойства событий**.
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 496

Экспорт событий в файл

► *Чтобы экспортировать события в файл:*

1. Запустите выборку событий (см. стр. 537).
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 496

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями (см. стр. 573), вы можете перейти к истории ревизий объекта.

► *Чтобы просмотреть историю объекта из события:*

1. Запустите выборку событий (см. стр. 537).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

См. также:

Сценарий: Мониторинг и отчеты 496

Удаление событий

► *Чтобы удалить одно или несколько событий:*

1. Запустите выборку событий (см. стр. 537).
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 496

kaspersky

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 **ОК**.

Выборка событий будет удалена.

См. также:

Сценарий: Мониторинг и отчеты 496

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 **Активы (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.

Блокировка частых событий

В этом разделе представлена информация об управлении блокировкой частых событий и об отмене блокировки частых событий.

В этом разделе

kaspersky

О блокировке частых событий

Управляемая программа, например Kaspersky Endpoint Security для Linux, 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. 165).

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. 543) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (на стр. 543) 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. 544) частых событий.

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.

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.

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 – 400000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Программа проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 00 больше указанного максимального значения, программа удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

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.

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. 546) 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. 552).

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 отчетность → 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.
- **Уведомления**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить программу безопасности на устройства, просмотреть список устройств или список событий (см. стр. 302). 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 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 **Больше**.

   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. 500).

   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. 502), 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 44. 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. • 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. • Приостановлена. • 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 подключался	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.
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. • Переключатель включен.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • 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
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). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен программой	Статус устройства определяется управляемой программой.	• Переключатель выключен. • Переключатель включен.
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. • Переключатель включен.
Выключена защита	Устройство видимо в сети, но программа безопасности на устройстве отключена больше указанного времени.	Более чем 0 минут.
Не запущена программа безопасности	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Переключатель выключен. • 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 данных 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 данных устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *ОК*.

См. также:

Настройка переключения статусов устройств 551

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 **Активы (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 **Активы (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:

Уведомления и статусы устройств 545

О статусах устройства 264

Сценарий: Мониторинг и отчеты 496

Сценарий: Настройка защиты сети 349

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 вкладке **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 **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес
- 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, 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 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.

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

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 **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 поле **Адрес электронной почты отправителя: Если этот параметр не указан, вместо него будет использоваться адрес получателя. Предупреждение: Не рекомендуется указывать в этом поле несуществующий адрес электронной почты**, 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 с подробными данными события (см. стр. 558).

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.

- **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
  - 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, 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 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 поле **Адрес электронной почты отправителя: Если этот параметр не указан, вместо него будет использоваться адрес получателя. Предупреждение: Не рекомендуется указывать в этом поле несуществующий адрес электронной почты**, 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, такие как имя события, имя устройства и имя домена (см. стр. 558).

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

По нажатию на кнопку **Отправить пробное сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения указанным получателям.

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

- **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, которые определяют сведения о событии, которые будут отправлены в сообщении (см. стр. 558). 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.

1. На закладке настройте параметры уведомлений.
2. 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. 369) для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах программы.

См. также:

Сценарий: Мониторинг и отчеты 496

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. Затем 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 тестовым "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.

► *Чтобы открыть запись об обнаружении тестового "вируса":*

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

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 45. Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события
%COMPUTER%	Имя устройства, на котором произошло событие
%DOMAIN%	Домен.
%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"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

kaspersky

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". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию (см. стр. 561).

  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. 330), 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 (см. стр. 561).

  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. 399).

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 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. 560), включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления. Если вы не хотите получать объявления, вы можете отключить эту функцию (см. стр. 561).

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" (см. стр. 559) 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" (см. стр. 559) (**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 безопасности [Включены]**.
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 вкладке **Общие** выберите раздел **Параметры прокси-сервера KSN**.
3. **Выключите параметр** Использовать Kaspersky Security Network [Включено]**.**
4. Нажмите на кнопку **Сохранить**.

   Объявления выключены.

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 настроить экспорт событий в SIEM-системы одним из следующих способов: экспорт в любую SIEM-систему, использующую формат Syslog, или экспорт событий в SIEM-системы непосредственно из базы данных 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. 564).
- Убедитесь, что у вас есть значения системных параметров (см. стр. 563).

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. 564).
- Выбор события, которые вы хотите экспортировать в SIEM-систему:

  Отметьте события, которые вы хотите экспортировать в SIEM-систему. Отметите общие события (см. стр. 568), которые возникают во всех управляемых программах "Лаборатории Касперского". Затем можно отметить события для экспорта для определенной управляемой программы (см. стр. 567).
- Настройка экспорта событий в SIEM-систему

  Экспортировать события можно сделать следующими способами:

  Укажите протоколы TCP/IP, UDP или TLS over TCP (см. стр. 569).

  Использование экспорта событий напрямую из базы данных Kaspersky Security Center (см. стр. 570). 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. 573), 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, 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

Kaspersky Security Center позволяет получать информацию о событиях (см. стр. 512), 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 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 программ 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 программы. 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.

Формат Syslog экспорта событий

Вы можете отправлять события в формате Syslog в любую SIEM-систему. В формате Syslog можно передавать любые события, произошедшие на Сервере администрирования и в программах "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий в формате Syslog можно выбирать, какие именно события будут переданы в SIEM-систему.

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.

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**

  Протокол передачи сообщений: UDP, TCP или TLS over TCP. Необходимо указать тот же протокол, который был выбран в Kaspersky Security Center для передачи событий.

- **Порт**

  Укажите номер порта для подключения к Kaspersky Security Center. Этот порт должен совпадать с портом, который вы указываете в Kaspersky Security Center при настройке экспорта событий в SIEM-систему (см. стр. 569).

- **Формат даты**

  Укажите формат Syslog.

В зависимости от используемой SIEM-системы может потребоваться указать дополнительные параметры приемника сообщений.

На рисунке ниже приведен пример настройки приемника в ArcSight.

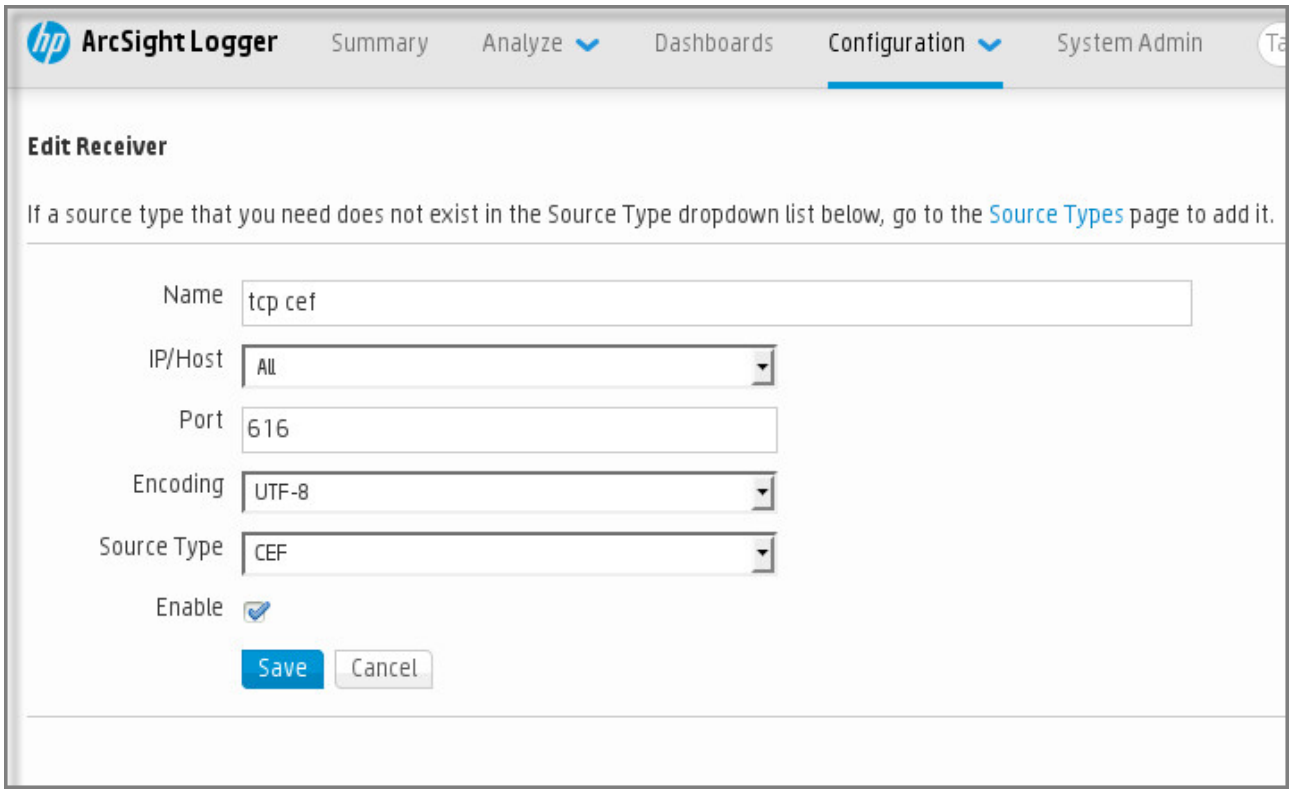


Рисунок 3. Пример настройки приемника сообщений

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 562

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.

См. также:

Сценарий: Настройка экспорта событий в SIEM-системы 562

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 562

kaspersky

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 **Активы (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 **Активы (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 512

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 **Активы (Устройства)** → **Политики и профили политик**, а затем перейдите по ссылке политики.
2. В открывшемся окне перейдите на закладку **Настройка событий**.
3. Нажмите **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 512

kaspersky

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 562

Настройка Kaspersky Security Center для экспорта событий в SIEM-систему

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky Security Center.

► *Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center Web Console:*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** 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**

5. Также можно экспортировать заархивированные события из базы данных Сервера администрирования и задать начальную дату, с которой вы хотите начать экспорт заархивированных событий:
   a. Перейдите по ссылке **Установите дату начала экспорта**.
   b. В открывшемся разделе укажите дату начала в поле **Дата начала экспорта**.
   c. Нажмите на кнопку **ОК**.
6. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы [Включено]**.
7. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует отмеченные события (см. стр. 566) в SIEM-систему. Если вы зададите дату начала экспорта, Сервер администрирования также экспортирует отмеченные события, хранящиеся в базе данных Сервера администрирования, начиная с указанной даты.

См. также:

О настройке экспорта событий в SIEM-системе 564

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.

См. также:

Создание SQL-запроса с помощью утилиты klsql2

В этом разделе приведены инструкции по использованию утилиты klsql2, а также по созданию SQL-запроса с использованием этой утилиты. Используйте версию утилиты klsql2, которая входит в вашу установленную версию Kaspersky Security Center.

► *Чтобы использовать утилиту klsql2:*

1. Перейдите в директорию /opt/kaspersky/ksc64/sbin/klsql2 на устройстве с установленным Сервером администрирования Kaspersky Security Center.
2. В этой директории создайте пустой файл src.sql.
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:

   ```
   sudo ./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 запроса.

Вы можете редактировать файл src.sql и создавать в нем любые запросы к публичным представлениям. Затем с помощью команды в командной строке можно запустить запрос и сохранить результаты в файл.

См. также

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 562

Просмотр имени базы данных Kaspersky Security Center

Для доступа к базе данных Kaspersky Security Center с помощью SQL Server, MySQL или MariaDB необходимо знать имя базы данных, чтобы иметь возможность подключиться к ней из редактора скриптов SQL.

► *Чтобы просмотреть имя базы данных Kaspersky Security Center:*

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 **Информация об используемой базе данных**.

Имя базы данных указано в поле **Имя базы данных**. 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 562

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.

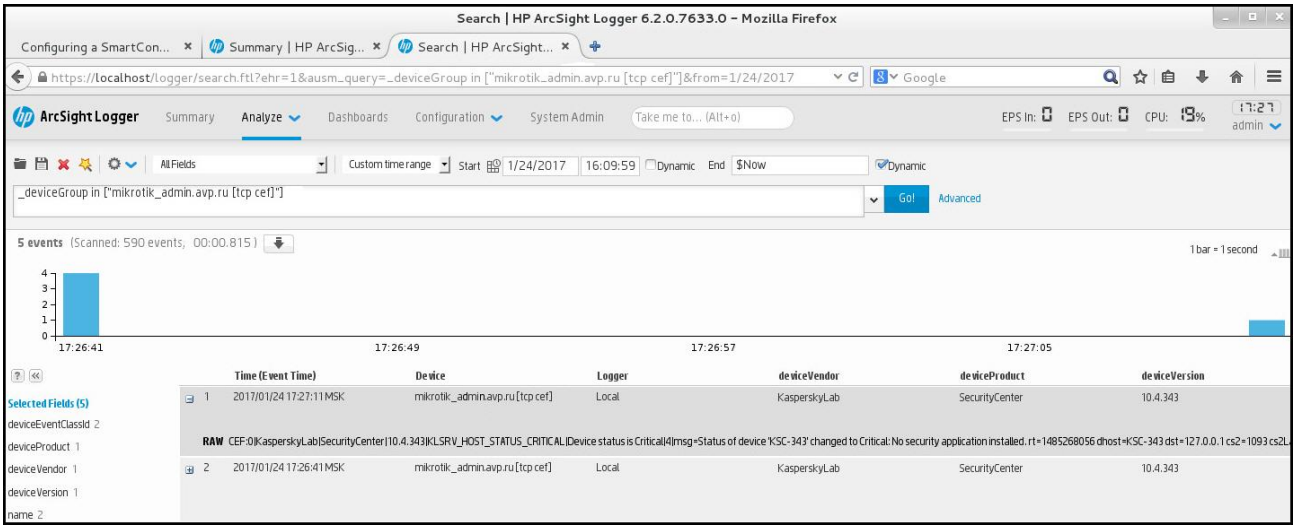


Рисунок 4. Пример событий

См. также:

Сценарий: Настройка экспорта событий в SIEM-системы 562

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.

В этом разделе

kaspersky

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;
- 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.

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 349

kaspersky

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 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** (см. стр. 445) 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, – остаются на устройстве.

Kaspersky Security Center обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств (см. стр. 245) 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.

  Правила хранения устройств не влияют на устройства, на которых один или несколько дисков зашифрованы с помощью полнодискового шифрования (см. стр. 292). Такие устройства не удаляются автоматически – вы можете удалить их только вручную. Если вам нужно удалить устройство с зашифрованным жестким диском, сначала расшифруйте диск, а затем удалите устройство.

  При удалении устройства с зашифрованным жестким диском данные, необходимые для расшифровки диска, также удаляются. В этом случае для расшифровки диска требуется выполнение следующих условий:

  Устройство повторно подключается к Серверу администрирования для восстановления данных, необходимых для расшифровки диска.

  Пользователь устройства помнит пароль для расшифровки.

  Программа безопасности, которая использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлена на устройстве.

  Если диск был зашифрован с помощью технологии Шифрование диска Kaspersky, вы также можете попробовать восстановить данные с помощью утилиты FDERT Restore https://support.kaspersky.com/KESWin/12.0/ru-RU/130941.htm.

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, 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.

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 Web Console.

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:*

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.

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".

kaspersky

Удаленная диагностика клиентских устройств

Вы можете использовать удаленную диагностику для удаленного выполнения следующих операций на клиентских устройствах на базе Windows и на базе Linux:

- включения и выключения трассировки, изменения уровня трассировки и загрузки файла трассировки;
- загрузки системной информации и параметров программы;
- загрузки журналов событий;
- создание файла дампа для программы;
- запуска диагностики и загрузки результатов диагностики;
- запуск, 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".

В этом разделе

kaspersky

Открытие окна удаленной диагностики

Чтобы выполнить удаленную диагностику клиентских устройств на базе Windows и на базе Linux, 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 **Активы (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 вкладку **Дополнительно**.
4. В появившемся окне нажмите на кнопку **Удаленная диагностика**.

   В результате открывается окно **Удаленная диагностика** клиентского устройства. Если отсутствует соединение между Сервером администрирования и клиентским устройством, появится сообщение об ошибке.

Если вам нужно получить сразу всю диагностическую информацию о клиентском устройстве с операционной системой Linux, вы можете запустить на этом устройстве скрипт collect.sh (см. стр. 586).

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. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.

   В разделе **Управление программами** откроется список программ "Лаборатории Касперского", установленных на устройстве.
3. В списке программ выберите программу, для которой требуется включить или выключить трассировку.

   Откроется список параметров удаленной диагностики.
4. 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.

   На клиентских устройствах под управлением Linux трассировка компонента Обновление Kaspersky Security Agent регулируется параметрами Агента администрирования. Поэтому параметры **Включить трассировку** и **Изменить уровень трассировки** выключены для этого компонента на клиентских устройствах под управлением Linux.

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, настроить или отключить трассировку Xperf:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.

   В разделе **Управление программами** откроется список программ "Лаборатории Касперского", установленных на устройстве.
3. В списке программ выберите Kaspersky Endpoint Security для Windows.

   Откроется список параметров удаленной диагностики для Kaspersky Endpoint Security для Windows.
4. В разделе **Трассировка Xperf** нажмите на кнопку **Включить трассировку Xperf**.

   Если трассировка Xperf уже включена, отображается кнопка **Выключить трассировку Xperf**. Нажмите на эту кнопку, если хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows.
5. 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 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.

   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 **Размер файлов ротации (МБ)**, 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.

6. Если вы хотите отключить трассировку Xperf для Kaspersky Endpoint Security для Windows, нажмите **Выключить трассировку Xperf** в разделе **Трассировка Xperf**.

   Трассировка Xperf выключена.

Загрузка файла трассировки программы

► *Чтобы загрузить файл трассировки программы:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.

   В разделе **Управление программами** откроется список программ "Лаборатории Касперского", установленных на устройстве.
3. В списке программ выберите программу, для которой вы хотите загрузить файл трассировки.
4. В разделе **Трассировка** нажмите на кнопку **Файлы трассировки**.

   Откроется окно **Журналы событий трассировки** устройства, где отображается список файлов трассировки.
5. В списке файлов трассировки выберите файл, который вы хотите загрузить.
6. Выполните одно из следующих действий:
   - Загрузите выбранный файл, нажав на кнопку **Загрузить**. Вы можете выбрать один или несколько файлов для загрузки.
   - Загрузите часть выбранного файла:
     a. Нажмите на кнопку **Загрузить часть**.

        Одновременная частичная загрузка нескольких файлов невозможна. Если вы выберете более одного файла трассировки, кнопка **Загрузить часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть файла для загрузки в соответствии с вашими требованиями.

        Для устройств под управлением Linux изменение имени части файла недоступно.

     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, выполните следующее действие:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В открывшемся окне удаленной диагностики выберите раздел **Журналы событий**.

3. В разделе **Файлы трассировки** нажмите **Журналы службы Центра обновления Windows** или **Журналы удаленной установки**, в зависимости от того, какие файлы трассировки вы хотите удалить.

   Ссылка **Журналы Центра обновления Windows** доступна только для клиентских устройств под управлением Windows.

   Откроется окно **Журналы событий трассировки** устройства, где отображается список файлов трассировки.

4. В списке файлов трассировки выберите один или несколько файлов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Выбранные файлы трассировки удалены.

Загрузка параметров программ

► *Чтобы загрузить с клиентского устройства параметры программ:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.
3. В разделе **Параметры программы** нажмите на кнопку **Загрузить** для загрузки информации о параметрах программ, установленных на клиентском устройстве.

ZIP-архив с информацией загрузится в указанное расположение.

Загрузка системной информации с клиентского устройства

► *Чтобы загрузить системную информацию с клиентского устройства выполните следующие действия:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В окне удаленной диагностики выберите раздел **Информация о системе**.
3. Нажмите на кнопку **Загрузить** для загрузки системной информации о клиентском устройстве.

   Если вы получаете системную информацию об устройстве под управлением Linux, в получившийся файл добавляется файл дампа для аварийно завершенных программ.

Файл с информацией загрузится в указанное расположение.

kaspersky

Загрузка журналов событий

► *Чтобы загрузить с удаленного устройства журнал событий:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В разделе **Журналы событий** в окне удаленной диагностики выберите **Журнал событий всех устройств**.
3. В окне **Журнал событий всех устройств** выберите один или несколько журналов 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**.

        Одновременная частичная загрузка нескольких журналов событий невозможна. Если вы выберете более одного журнала событий, кнопка **Загрузить часть** будет неактивна.

     b. В открывшемся окне укажите имя и часть журнала событий для загрузки в соответствии с вашими требованиями.

        Для устройств под управлением Linux изменение имени части журнала событий недоступно.

     c. Нажмите на кнопку **Загрузить**.

Выбранный журнал событий или его часть загрузится в указанное расположение.

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. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.

   В разделе **Управление программами** откроется список программ "Лаборатории Касперского", установленных на устройстве.
3. В списке программ выберите программу, которую вы хотите запустить, остановить или перезапустить.
4. 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. 579).
2. В окне удаленной диагностики выберите раздел **Программы "Лаборатории Касперского"**.

   В разделе **Управление программами** откроется список программ "Лаборатории Касперского", установленных на устройстве.
3. В списке программ выберите программу, для которой вы хотите запустить удаленную диагностику.

   Откроется список параметров удаленной диагностики.
4. 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 о диагностике** становится доступной.
5. Нажмите на кнопку **Загрузить отчет диагностики**, чтобы загрузить отчет.

Отчет загрузится в указанное расположение.

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. 579).
2. В окне удаленной диагностики выберите раздел **Запуск удаленной программы**.
3. В разделе **Файлы программы** нажмите на кнопку **Обзор** для выбора ZIP-архива с программой, которую вы хотите запустить на клиентском устройстве.

   ZIP-архив должен содержать папку утилиты. Эта папка содержит исполняемый файл для запуска на удаленном устройстве.

   При необходимости можно указать имя исполняемого файла и аргументы командной строки. Для этого заполните поля **Исполняемый файл в архиве для запуска на удаленном устройстве** и **Аргументы командной строки**.

4. Нажмите на кнопку **Загрузить и запустить** для запуска указанной программы на клиентском устройстве.
5. Следуйте указаниям сотрудника службы поддержки "Лаборатории Касперского".

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 клиентских устройств под управлением Linux и для 64-битных процессов эта функция не поддерживается.

► *Чтобы создать файл дампа для программы:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 579).
2. В окне удаленной диагностики выберите раздел **Запуск удаленной программы**.
3. В разделе **Формирование дампа процесса** укажите исполняемый файл программы, для которой вы хотите создать файл дампа.
4. Нажмите на кнопку **Загрузить**, чтобы сохранить файл дампа указанной программы.

   Если указанная программа не запущена на клиентском устройстве, отобразится сообщение об ошибке.

Запуск удаленной диагностики на клиентском устройстве с операционной системой Linux

Kaspersky Security Center позволяет загружать основную диагностическую информацию с клиентского устройства (см. стр. 578). Кроме того, вы можете получить диагностическую информацию об устройстве с операционной системой Linux с помощью скрипта collect.sh "Лаборатории Касперского". Этот скрипт запускается на клиентском устройстве с операционной системой Linux, которое необходимо диагностировать. Затем создается файл с диагностической информацией, системной информацией об этом устройстве, файлами трассировки программ, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных программ.

Рекомендуется использовать скрипт collect.sh для получения сразу всей диагностической информации о клиентском устройстве с операционной системой Linux. Если вы загружаете диагностическую информацию удаленно через Kaspersky Security Center, вам нужно будет пройти все разделы интерфейса удаленной диагностики (см. стр. 579). Кроме того, диагностическая информация для устройства с операционной системой Linux, вероятно, не будет получена полностью.

Если вам необходимо отправить сформированный файл с диагностической информацией в Службу технической поддержки "Лаборатории Касперского", удалите всю конфиденциальную информацию перед отправкой файла.

► *Чтобы загрузить диагностическую информацию с клиентского устройства с операционной системой Linux с помощью скрипта collect.sh:*

1. Загрузите скрипт collect.sh, который запакован в архив collect.tar.gz https://box.kaspersky.com/f/00a1a6d8beb24554a72d?_ga=2.227118109.1421819605.1691580180-1314822200.1681888137.
2. Скопируйте загруженный архив на клиентское устройство с операционной системой Linux, которое необходимо диагностировать.
3. Выполните следующую команду, чтобы распаковать архив collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Выполните следующую команду, чтобы указать права на выполнение скрипта:

   ```
   # chmod +x collect.sh
   ```

5. Запустите сценарий collect.sh под учетной записью с правами администратора:

   ```
   # ./collect.sh
   ```

Файл с диагностической информацией будет сформирован и сохранен в папке /tmp/$HOST_NAME-collect.tar.gz.

kaspersky

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

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 Linux компонент Контроль программ доступен, начиная с Kaspersky Endpoint Security 11.2 для Linux.

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows создана и активна.

Этапы

Сценарий использования компонента Контроль программ состоит из следующих этапов:

1. 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.

Инструкция: Получение и просмотр списка программ, установленных на клиентских устройствах (см. стр. 591).

q. 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.

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах (см. стр. 592)

r. 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 двух типов.

Инструкция: Создание пополняемой вручную категории программ (см. стр. 593), Создание категории программ, в которую входят исполняемые файлы с выбранных устройств (см. стр. 596).

s. Настройка компонента Контроль программ в политике Kaspersky Endpoint Security

Настройте компонент Контроль программ в политике Kaspersky Endpoint Security для Linux с использованием категорий программ, которые вы создали на предыдущем этапе.

Инструкция: Настройка компонента Контроль программ в политике Kaspersky Endpoint Security для Windows (см. стр. 598).

t. 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 Web Console: Настройка компонента Контроль программ в политике Kaspersky Endpoint Security для Windows (см. стр. 598). Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

u. 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 для Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию программы (см. стр. 600).

v. **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 Web Console: Настройка компонента Контроль программ в политике Kaspersky Endpoint Security для Windows (см. стр. 598). Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

w. **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.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows Help https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.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 версии программы Kaspersky Endpoint Security 11.2 для Linux и выше.

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 два типа категорий программ:

- Пополняемая вручную категория. (см. стр. 593) Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, путь к файлу, чтобы включить исполняемые файлы в категорию.
- Категория, в которую входят исполняемые файлы с выбранных устройств (см. стр. 596). Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows Help https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.htm.

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.

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 столбцов** 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.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows Help https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.htm.

См. также:

Сценарий: Управление программами 588

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 программы Kaspersky Endpoint Security для Linux версии 11.2 и выше.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:*

1. В главном окне программы перейдите к закладке **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи (см. стр. 408). Следуйте далее указаниям мастера.

3. На странице **Новая задача** в раскрывающемся списке **Программа** выберите Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows 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 онлайн-справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/219385.htm и Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/222859.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.

См. также:

Сценарий: Управление программами 588

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**, укажите имя категории программ и выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.

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 для Linux поддерживает вычисление SHA-256.

    Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

    - Если все экземпляры программ безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA-256**.
    - Установите флажок **MD5 hash**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает

хеш-функцию MD5.

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 архивной папки**

  Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления программ в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA-256) вы хотите использовать для вычисления значения хеш-функции. Программы, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию программ.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления программ в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

- **Хеш файла**

  Вы можете выбрать, какую хеш-функцию (MD5 или SHA-256) вы хотите использовать для вычисления значения хеш-функции. Программы, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию программ.

  Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

  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.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows Help https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.htm.

См. также:

Сценарий: Управление программами 588

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. Следуйте далее указаниям мастера.

3. На странице мастера **Выбор способа создания категории,** укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы обрабатываются автоматически, их метрики заносятся в категорию**.
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 для Linux поддерживает вычисление SHA-256.

  Выберите один из вариантов вычисления хеш-функции программой Kaspersky Security Center для файлов категории:

  - Если все экземпляры программ безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA-256**.

  Установите флажок **MD5 hash**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

  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 588

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 588

Настройка компонента Контроль программ в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля программ, 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 **Активы (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. Выключите переключатель **Контроль Программ [Выключен]**, чтобы выключить параметр.

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 вкладка **Список запрещенных**, если выбран режим **Список запрещенных** или отображается вкладка **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 **OK**.

    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 **OK**, чтобы сохранить параметры и закрыть окно **Правило Контроля программ**.
16. Нажмите на кнопку **OK**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.
17. Нажмите на кнопку **OK**, 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.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows Help https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.htm.

См. также:

Сценарий: Управление программами 588

Добавление исполняемых файлов, связанных с событием, в категорию программы

После настройки компонента Компонента Контроль программ в политиках Kaspersky Endpoint Security 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. 536) 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. 537).

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 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)**

Выберите этот параметр, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

1. 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.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/ и Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.0/ru-RU/127971.htm.

См. также:

Сценарий: Управление программами 588

Изменение языка интерфейса Kaspersky Security Center Web Console

Вы можете выбрать язык интерфейса Kaspersky Security Center Web Console.

► *Чтобы изменить язык интерфейса:*

1. В главном окне программы перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.

kaspersky

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную. 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. Используя OpenAPI, вы можете разработать клиентскую программу.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI
https://support.kaspersky.com/help/KSC/15/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. 52), запускать задачи (см. стр. 59) в Kaspersky Security Center или назначать точки распространения (см. стр. 62). 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/15/KSCAPI/common/KlAkOAPI-15.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 из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования https://support.kaspersky.com/help/KSC/15/KSCAPI/a00444.html.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

Таблица 46. Сопоставление пользовательских сценариев и примеров методов Kaspersky Security Center OpenAPI

Пример	Назначение примера	Сценарий
Log KlAkParams https://support.kaspersky.com/help/KSC/15/KSCAPI/a00427.html	Вы можете извлекать и обрабатывать данные с помощью структуры данных `KlAkParams`. В примере показано, как работать с этой структурой данных. Пример вывода может быть представлен по-разному. Вы можете получить данные для отправки HTTP-метода или использовать их в своем коде.	Мониторинг и отчеты

Пример	Назначение примера	Сценарий
Создание и удаление первичного/вторичного отношения https://support.kaspersky.com/help/KSC/15/KSCAPI/a0042 8.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. 155) и удаление иерархии Серверов администрирования (см. стр. 170).
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство https://support.kaspersky.com/help/KSC/15/KSCAPI/a0043 1.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 64), а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений (см. стр. 253)
Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования https://support.kaspersky.com/help/KSC/15/KSCAPI/a0043 2.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
Создайте отчет об эффективных правах пользователей https://support.kaspersky.com/help/KSC/15/KSCAPI/a0043 3.html	Вы можете создать разные отчеты https://support.kaspersky.com/help/KSC/15/KSCAPI/a0003 2.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. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета (см. стр. 510)
Запустите задачу на устройстве https://support.kaspersky.com/help/KSC/15/KSCAPI/a0043 4.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 64), а затем запустить необходимую задачу.	Запустите задачу вручную (см. стр. 409).

Пример	Назначение примера	Сценарий
Регистрация точек распространения для устройств в группе https://support.kaspersky.com/help/KSC/15/KSCAPI/a00436.html	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и программ "Лаборатории Касперского" (см. стр. 468)
Перечисление всех групп https://support.kaspersky.com/help/KSC/15/KSCAPI/a00437.html	Вы можете выполнять различные действия с группами администрирования. В примере показано, как выполнить следующее: • Получить идентификатор корневой группы "Управляемые устройства". • Переместить по иерархии групп. • Получить полную развернутую иерархию групп с их именами и вложенностью.	Настройка Сервера администрирования (см. стр. 152)
Перечисление задач, запрос статистики задач и запуск задач https://support.kaspersky.com/help/KSC/15/KSCAPI/a00438.html	Вы можете ознакомиться со следующей информацией: • Историей выполнения задачи. • Текущим статусом задачи. • Количеством задач в разных статусах. Вы также можете запустить задачу. По умолчанию пример запускает задачу после вывода статистики.	Наблюдение за ходом выполнения задачи
Создание и запуск задачи https://support.kaspersky.com/help/KSC/15/KSCAPI/a00439.html	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Имя. • Группа устройств, для которой будет использоваться задача. 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/15/KSCAPI/a00030.html.	Создание задачи
Перечисление лицензионных ключей https://support.kaspersky.com/help/KSC/15/KSCAPI/a00440.html	Вы можете получить список всех активных лицензионных ключей для программ "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения https://support.kaspersky.com/help/KSC/15/KSCAPI/a00117.html о каждом лицензионном ключе, такие как имя, тип или срок действия.	Просмотр информации об используемых лицензионных ключах

Пример	Назначение примера	Сценарий
Создание и поиск внутреннего пользователя https://support.kaspersky.com/help/KSC/15/KSCAPI/a00441.html	Вы можете создать учетную запись для дальнейшей работы.	Выбор учетной записи для запуска Сервера администрирования
Создание пользовательской категории https://support.kaspersky.com/help/KSC/15/KSCAPI/a00442.html	Вы можете создать категорию программ с требуемыми параметрами https://support.kaspersky.com/help/KSC/15/KSCAPI/a00450.html.	Создание пополняемой вручную категории программ (см. стр. 593)
Перечисление пользователей с помощью SrvView https://support.kaspersky.com/help/KSC/15/KSCAPI/a00443.html	Вы можете использовать класс SrvView https://support.kaspersky.com/help/KSC/15/KSCAPI/a00582.html для запроса подробной информации https://support.kaspersky.com/help/KSC/15/KSCAPI/a00154.html с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление учетными записями пользователей

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. 153) 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

Руководство по масштабированию

В этом онлайн-руководстве представлена информация по масштабированию Kaspersky Security Center: https://help.kaspersky.com/KSCLinux/15/ru-RU/162088.htm.

См. также:

Начало работы 78

kaspersky

Устранение уязвимостей и установка критических обновлений в программе

"Лаборатория Касперского" может выпускать обновления программы, направленные на устранение уязвимостей и недостатков безопасности (критические обновления). Срочные пакеты обновлений публикуются на серверах автоматизированной установки обновлений "Лаборатории Касперского". Уведомления о выпуске критических обновлений публикуются на веб-сайте (https://support.kaspersky.ru/general/certificates) и рассылаются по адресам электронной почты, указанным при заказе программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке: http://support.kaspersky.ru/subscribe).

Порядок получения критических обновлений изложен в формуляре.

Лицо, ответственное за эксплуатацию программы, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в программе, используя веб-сайт "Лаборатории Касперского" (https://support.kaspersky.ru/vulnerability), банк данных угроз безопасности информации ФСТЭК России (http://www.bdu.fstec.ru) и иные общедоступные источники.

Вы можете сообщать об обнаруженных недостатках безопасности или уязвимостях программы следующими способами:

- Через веб-форму на веб-сайте Службы технической поддержки (https://support.kaspersky.ru/vulnerability.aspx?el=12429).
- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского".

kaspersky

Действия после сбоя или неустранимой ошибки в работе программы

Программа автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда программа не может восстановить свою работу, вам требуется переустановить программу или ее компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. стр. 611).

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

Известные ошибки и ограничения

Kaspersky Security Center 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 список содержит более 20 записей, которые отображаются на нескольких страницах, и вы установили флажок **Выбрать все**, Web Console выбирает только те записи, которые отображаются на текущей странице. Обратите внимание, что это не относится к спискам в разделах **Управляемые устройства**, **Выборки устройств** и **Задачи**, где можно выбрать все элементы из списка.
- В политике Kaspersky Endpoint Security для Windows в разделе **Контроль программ** после выбора категории программы и сохранения политики категория программы не отображается как выбранная в политике.
- После установки Kaspersky Industrial CyberSecurity for Linux Nodes эта программа не отображается в окне свойств устройства.
- В политике для Kaspersky Endpoint Security для Linux некорректно отображается список пользователей при создании правила Контроль программ.
- Когда служба прокси-сервера KSN выключена, управляемые устройства в подгруппе не отправляют статус "Серверы KSN недоступны".
- В отчетах с буквенным форматом разрыв страницы может обрезать строку текста по горизонтали.
- 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.
- Если в мастере **Добавить подчиненный Сервер администрирования** 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 отключена двухэтапная проверка, или создайте иерархию из будущего подчиненного Сервера.
- Если вы открываете Kaspersky Security Center 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".
- Информация об оборудовании, отправляемая с управляемого устройства на Сервер администрирования, может быть неполной; некоторое оборудование может быть не указано.

- 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.
- В 64-разрядной версии Astra Linux пакет klnagent-astra нельзя обновить с помощью пакета klnagent64_14: старый пакет klnagent64-astra будет удален, а вместо обновления будет установлен новый пакет klnagent64, поэтому будет добавлен новый значок для устройства с пакетом klnagent64_14. Вы можете удалить старый значок для этого устройства.

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. Консоль администрирования является аналогом Kaspersky Security Center Web Console.

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 Kaspersky Security Center 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 вы открываете Kaspersky Security Center 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".

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.

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).

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.

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.

kaspersky

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

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.

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

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.

kaspersky

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

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

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.

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.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии.

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.

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.

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

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.

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. 616).

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

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).

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.

Adobe, Acrobat, Flash, Shockwave, PostScript являются либо зарегистрированными товарными знаками, либо товарными знаками компании Adobe в США и/или других странах.

AMD, AMD64 – товарные знаки или зарегистрированные товарные знаки Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace – являются товарными знаками Amazon.com, Inc. или аффилированных лиц компании.

Apache и Apache feather logo – товарные знаки Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, Touch ID – товарные знаки Apple Inc.

Arm – зарегистрированный товарный знак Arm Limited (или дочерних компаний) в США и/или других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Ubuntu, LTS являются зарегистрированными товарными знаками Canonical Ltd.

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.

Corel – товарный знак или зарегистрированный в Канаде, Соединенных Штатах Америки и в других странах товарный знак Corel Corporation и/или ее дочерних компаний.

Cloudflare, логотип Cloudflare и Cloudflare Workers являются товарными знаками и/или зарегистрированными товарными знаками компании Cloudflare, Inc. в США и других юрисдикциях.

Dropbox – товарный знак Dropbox, Inc.

Знак Firebird является зарегистрированным товарным знаком фонда Firebird.

Foxit – зарегистрированный товарный знак Foxit Corporation.

Знак FreeBSD является зарегистрированным товарным знаком фонда FreeBSD.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts, YouTube – товарные знаки Google LLC.

EulerOS, FusionCompute, FusionSphere – товарные знаки Huawei Technologies Co., Ltd.

Intel, Core, Xeon – товарные знаки Intel Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

IBM, QRadar – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Node.js – товарный знак Joyent, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

kaspersky

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista, Windows Azure – являются товарными знаками группы компаний Microsoft.

Mozilla, Firefox, Thunderbird – товарные знаки Mozilla Foundation, зарегистрированные в США и других странах.

Novell – товарный знак Novell Enterprises Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

Oracle, Java, JavaScript, TouchDown – зарегистрированные товарные знаки Oracle Corporation и/или ее аффилированных компаний.

Parallels, логотип Parallels и Coherence являются товарными знаками или зарегистрированными товарными знаками Parallels International GmbH.

Chef – товарный знак или зарегистрированный в США и/или других странах товарный знак Progress Software Corporation и/или одной из дочерних или аффилированных компаний.

Puppet – товарный знак или зарегистрированный товарный знак компании Puppet, Inc.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Red Hat, Fedora, Red Hat Enterprise Linux – товарные знаки Red Hat Inc., зарегистрированные в Соединенных Штатах Америки и в других странах.

Ansible является зарегистрированным товарным знаком Red Hat, Inc. в США и других странах.

CentOS – товарный знак Red Hat Inc., зарегистрированный в Соединенных Штатах Америки и в других странах.

BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Splunk, SPL – товарные знаки и зарегистрированные в США и других странах товарные знаки Splunk, Inc.

SUSE – зарегистрированный в США и других странах товарный знак SUSE LLC.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

OpenAPI – товарный знак Linux Foundation.

VMware, VMware vSphere, VMware Workstation – товарные знаки или зарегистрированные в США или других юрисдикциях товарные знаки VMware, Inc.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.

kaspersky

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 47. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
программа	продукт, объект оценки, программное изделие
вирус, программа, представляющая угрозу, вредоносная программа	КВ, компьютерный вирус
антивирусные базы, базы программы	базы данных признаков компьютерных вирусов (БД ПКВ)
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

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 сертифицированной конфигурации на другие значения выводит программу из безопасного состояния.

Сертифицированная конфигурация программы не включает в себя функциональность Kaspersky XDR Expert.

Таблица 48. 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.	
Автоматическое обновление модулей Агентов администрирования	Обновления модулей Агента администрирования устанавливаются автоматически, после того как Сервер администрирования завершает задачу получения обновлений. Возможные значения: • включен; • 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. Возможные значения: • включен; • выключен.	Выключен.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Запуск задачи **Загрузка обновлений в хранилище Сервера администрирования**	Задача **Загрузка обновлений в хранилище Сервера администрирования** выполняет загрузку обновлений баз и программных модулей, которые копируются с источника обновлений и размещаются в папке общего доступа. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически по расписанию с интервалом один раз в час.
Запуск задачи **Установка обновлений**	Задача **Установка обновлений** выполняет установку ранее загруженных в хранилище обновлений на клиентские устройства. Возможные значения: • вручную; • автоматически по расписанию.	Автоматически, по завершении задачи **Загрузка обновлений в хранилище Сервера администрирования**.
Источник обновлений задачи **Загрузка обновлений в хранилище Сервера администрирования**	Источник обновлений баз и модулей управляемых программ "Лаборатории Касперского". Возможные значения: • серверы обновлений "Лаборатории Касперского"; • главный Сервер Администрирования; • локальная или сетевая папка.	• Главный Сервер Администрирования; • локальная или сетевая папка. Источник обновлений *Серверы обновлений "Лаборатории Касперского"* удален, чтобы программа не передавала информацию на серверы обновлений "Лаборатории Касперского".
Способ активации Сервера администрирования	Возможные значения: • с помощью файла ключа; • с помощью кода активации.	С помощью файла ключа.
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". Возможные значения: • отключена; • включена.	Отключена.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
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. Возможные значения: • используется; • 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 **Обнаружено много вирусов** со значением **Более 0**.
Отправка уведомлений по электронной почте	Отправка уведомлений нужна для оповещения о событиях и для того, чтобы вы могли быстрее отреагировать на произошедшие события и выполнить действия, которые считаете подходящими. В настройках политики Kaspersky Endpoint Security для Linux и свойствах Сервера администрирования можно выбрать одно из возможных значений отправки уведомлений: • отключена; • включена.	Включена.
Максимальное количество событий, хранящихся в базе данных Сервера администрирования	Максимальное количество событий, которое хранится в базе данных Сервера администрирования, необходимое для проведения аудита программы.	Не меньше 400 000 событий.
Срок хранения событий	Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита программы.	Для событий с уровнем важности: • *Критические* – не меньше 180 дней. • *Отказ функционирования* – не меньше 180 дней. • *Предупреждение* – не меньше 90 дней. • *Информационное сообщение* – не меньше 30 дней.

Параметр	Краткое описание и диапазон значений	Значение параметра для программы в сертифицированном состоянии
Срок хранения ревизий изменений объектов	Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита программы.	Не меньше 90 дней.
Объявления "Лаборатории Касперского"	Объявления "Лаборатории Касперского" предоставляют информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах.	Отключены.
Максимальное количество попыток ввода пароля для подключения пользователя к Kaspersky Security Center 14 Linux	Если пользователь неправильно вводит пароль от своей учетной записи максимальное количество раз, учетная запись блокируется на один час.	Не больше 10 попыток.
Параметр **Сохранять все события** в свойствах задачи **Антивирусная проверка** программы Kaspersky Endpoint Security для Linux, если она установлена	Если параметр включен, в базе данных Сервера администрирования сохраняются результаты всех антивирусных проверок, выполненных на управляемых устройствах с помощью Kaspersky Endpoint Security для Linux. По умолчанию результаты хранятся в течение 7 дней. Возможные значения: • отключен; • включен.	Включен.
Порт 13291	Порт используется для подключений Консоли администрирования к Серверу администрирования. По умолчанию пользователи работают в Kaspersky Security Center 14 Linux через Kaspersky Security Center 14 Web Console. Поэтому порт 13291 по умолчанию закрыт. У вас есть возможность работать в Консоли администрирования на основе консоли управления Microsoft Management Console (MMC) вместо Kaspersky Security Center 14 Web Console. Для этого нужно открыть порт 13291. Возможные значения: • порт открыт; • порт закрыт.	Закрыт. Работа в Консоли администрирования не соответствует сертифицированному состоянию Kaspersky Security Center 14 Linux, поэтому порт должен остаться закрытым.

kaspersky

Настройка эталонных значений

Этот раздел содержит инструкции по установке эталонных значений параметров программы Kaspersky Security Center. 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, выполните следующие действия:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На закладке **Общие** выберите **Папка общего доступа Сервера администрирования**.
3. В поле **Путь к папке общего доступа** измените расположение папки общего доступа.

Расположение **Папки общего доступа Сервера администрирования** изменится на указанное.

Политики

Необходимо создать политики для программы Агента администрирования и управляемых программ, таких как Kaspersky Endpoint Security для Linux. Создайте политики, как описано в инструкции (см. стр. 367).

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, выполните следующие действия:

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"**.

   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*.
5. Нажмите на кнопку **Сохранить**.

Автоматическая установка патчей "Лаборатории Касперского" со статусом одобрения *Не определено* отключена.

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, выполните следующие действия:*

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**, выполните следующие действия:*

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.

Источник обновлений задачи Загрузка обновлений в хранилище Сервера администрирования 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, выполните следующие действия:*

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** нажмите на кнопку **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, выполните следующие действия:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. Выберите закладку **Общие** → **Лицензионные ключи**.
3. В поле **Действующая лицензия** укажите файл ключа, на основании которого ключ будет добавлен в программу.
4. 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", выполните следующие действия:*

1. На устройстве Сервера Администрирования запустите командную строку Linux.

2. Выполните следующие команды:
   - Для остановки службы: `sudo systemctl stop klactprx_svc`
   - Для выключения службы: `sudo systemctl disable klactprx_svc`

Служба прокси-сервера активации "Лаборатории Касперского" остановлена и выключена.

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, выполните следующие действия:*

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, выполните следующие действия:*

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. На странице **Определение области** в мастере выберите группу администрирования, которую требуется добавить в область роли.
6. Нажмите на кнопку **Назначить роль**.

В результате роль с набором прав на работу с Сервером администрирования будет назначена пользователю или группе пользователей. Назначенные роли отображаются на закладке **Права доступа** 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, выполните следующие действия:*

1. В разделе **Устройства** выберите **Иерархия групп**.
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 **Условие** выберите и установите переключатель для условия **Обнаружено много вирусов**.
5. Нажмите на кнопку **Изменить**.
6. Для условия **Обнаружено много вирусов** установите значение 1.
7. Нажмите на кнопку **ОК**.

Изменение статуса устройства на *Критический*, при обнаружении на нем хотя бы одного вируса, настроено.

Отправка уведомлений по электронной почте

Отправка уведомлений нужна для оповещения о событиях и для того, чтобы вы могли быстрее отреагировать на произошедшие события и выполнить действия, которые считаете подходящими.

► *Чтобы настроить и включить отправку уведомлений по электронной почте:*

1. В окне свойств Сервера администрирования включите и настройте отправку уведомлений по электронной почте как описано в инструкции (см. стр. 552).

   По умолчанию Kaspersky Endpoint Security для Linux для отправки уведомлений по электронной почте использует параметры, установленные в окне свойств Сервера администрирования. Вы можете изменить эту настройку в политике Kaspersky Endpoint Security для Linux.
2. В разделе **Устройства** выберите раздел **Политики и профили политик**.
3. Выберите политику **Kaspersky Endpoint Security для Linux**.

   Откроется окно свойств политики.
4. В окне свойств политики перейдите в раздел **Настройка событий**.

   Все события разделены по степени важности и перечислены в следующих разделах: **Критическое**, **Отказ функционирования**, **Предупреждение**, **Информационное сообщение**.

5. Перейдите в требуемый раздел и нажмите на кнопку **Добавить событие**.
6. Установите флажки рядом с теми сообщениями, уведомления для которых вы хотите получать, и нажмите на кнопку **ОК**.

Отправка уведомлений по электронной почте настроена.

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, выполните следующие действия:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На закладке **Общие** выберите **Хранилище событий**.
3. 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, выполните следующие действия:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. Выберите закладку **Настройка событий**.
3. 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 и установите необходимое значение (не меньше 90 дней).
   - На закладке **Информационное сообщение** выберите нужное событие и установите необходимое значение (не меньше 30 дней).
4. 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, выполните следующие действия:*

1. В разделе **Устройства** выберите раздел **Политики и профили политики**.
2. В поле **Имя политики** выберите политику Сервера администрирования.

   Откроется окно свойств политики.
3. 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 ревизий изменений объектов

Необходимо настроить срок хранения ревизий объектов, необходимый для проведения аудита программы. Рекомендуемый срок хранения ревизий изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита программы.

► *Чтобы изменить срок хранения ревизий изменения объектов:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На закладке **Общие** выберите раздел **Хранилище истории ревизий**.
3. В поле **Срок хранения ревизии изменения объекта** установите значение не меньше 90.
4. Нажмите на кнопку **Сохранить**.

Срок хранения ревизий изменения объектов изменен.

Выключение объявлений, связанных с безопасностью

Выключите объявления "Лаборатории Касперского", связанные с безопасностью, как описано в инструкции (см. стр. 561).

Максимальное количество попыток ввода пароля для подключения пользователя к Kaspersky Security Center

Установите максимальное количество попыток ввода пароля, как описано в инструкции (см. стр. 463). Рекомендуется установить значение не больше 10 попыток.

Сохранение результатов антивирусных проверок

В свойствах задачи **Поиск вирусов** необходимо включить параметр для сохранения в базе данных Сервера администрирования результатов всех антивирусных проверок, выполненных на управляемых устройствах с помощью Kaspersky Endpoint Security для Linux.

► *Чтобы включить параметр для сохранения результатов антивирусных проверок:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Поиск вирусов**, которая относится к программе Kaspersky Endpoint Security для Linux.

   Откроется окно свойств задачи.
3. В окне задачи выберите раздел **Параметры**.
4. Выберите раздел **Уведомления** и нажмите на кнопку **Параметры**.

   Откроется окно параметров.
5. Выберите параметр **Сохранять все события**, установите флажок **Хранить в базе данных Сервера администрирования в течение** и затем укажите срок, в течение которого необходимо хранить события.
6. Нажмите на кнопку **ОК** и затем на кнопку **Сохранить**.

Сохранение результатов антивирусных проверок включено.

Закрытие порта 13291

Порт используется для подключений Консоли администрирования к Серверу администрирования. По умолчанию пользователи работают в Kaspersky Security Center через Kaspersky Security Center Web Console. Работа в Консоли администрирования не соответствует сертифицированному состоянию Kaspersky Security Center, поэтому порт должен остаться закрытым.