kaspersky

Kaspersky Security Center (для Linux)

Подготовительные процедуры и руководство по эксплуатации

Версия приложения:15.1.0.12199

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: 31.05.2024

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", "приложение").

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

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

В документе также содержатся разделы с дополнительной информацией о приложении.

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 приложении

Указанные источники информации о приложении (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 приложении, его 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/ksc-linux/15 вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании приложения.

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

Для отображения справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. стр. 735).

kaspersky

Требования

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

В этом разделе

Указания по эксплуатации и требования к среде

1. Установка, конфигурирование и управление приложением должны осуществляться в соответствии с эксплуатационной документацией.
2. Приложение должно эксплуатироваться на компьютерах, отвечающих минимальным требованиям, приведенным в разделе "Аппаратные и программные требования".
3. Перед установкой и началом эксплуатации приложения необходимо установить все доступные обновления для используемых версий ПО среды функционирования.
4. Должен быть обеспечен доступ приложения ко всем объектам информационной системы, которые необходимы приложению для реализации своих функциональных возможностей (к контролируемым объектам информационной системы).
5. Должна быть обеспечена совместимость приложения с контролируемыми ресурсами информационной системы.
6. Должна быть обеспечена возможность корректной совместной работы приложения 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 установлено приложение.
8. Должна быть обеспечена синхронизация по времени между компонентами приложения, а также между приложением и средой его функционирования.
9. Персонал, ответственный за функционирование приложения, должен обеспечивать надлежащее функционирование приложения, руководствуясь эксплуатационной документацией.
10. Должна быть обеспечена доверенная связь между приложением и уполномоченными субъектами информационной системы (администраторами безопасности).
11. Функционирование приложения должно осуществляться в среде функционирования, предоставляющей механизмы аутентификации и идентификации администраторов безопасности приложения.
12. Должен быть обеспечен доверенный канал получения обновлений БД ПКВ.
13. Должна быть обеспечена защищенная область для выполнения функций безопасности приложения.
14. Управление атрибутами безопасности, связанными с доступом к функциям и данным приложения, должно предоставляться только уполномоченным ролям (администраторам приложения 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.

Аппаратные и программные требования

Сервер администрирования

Kaspersky Security Center Web Console

Агент администрированвания 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 12 (Bookworm) 64-разрядная.
- Debian GNU/Linux 11.x (Bullseye) 64-разрядная.
- Debian GNU/Linux 10.x (Buster) 64-разрядная.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
- CentOS 7.x 64-разрядная.
- CentOS Stream 9 64-разрядная.
- Red Hat® Enterprise Linux Server 9.x 64-разрядная.
- Red Hat Enterprise Linux Server 8.x 64-разрядная.
- Red Hat Enterprise Linux Server 7.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.10015-03 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-37 64-разрядная.
- Альт СП 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.
- Альт СП Рабочая станция 10 64-разрядная.
- Альт Рабочая станция 10 64-разрядная.
- Oracle® Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Oracle Linux 9 64-разрядная.
- Platform V SberLinux OS Server (SLO) 8.8 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 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.
- Parallels Desktop 18.
- 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 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.

- MariaDB 10.11 (сборка 10.11.3 и выше) 32-разрядная/64-разрядная.
- MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- PostgreSQL 13.x 64-разрядная.
- PostgreSQL 14.x 64-разрядная.
- 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.
- Jatoba 4 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 12 (Bookworm).
- Debian GNU/Linux 11.x (Bullseye).
- Ubuntu Server 22.04 LTS (Jammy Jellyfish).
- Ubuntu Server 20.04 LTS (Focal Fossa).
- CentOS Stream 9.
- Red Hat Enterprise Linux Server 9.x.
- Red Hat Enterprise Linux Server 8.x.
- Red Hat Enterprise Linux Server 7.x.
- SUSE Linux Enterprise Server 12 (все пакеты обновлений).
- SUSE Linux Enterprise Server 15 (все пакеты обновлений).
- Astra Linux Special Edition РУСБ.10015-03.

- Astra Linux Special Edition РУСБ.10015-37 (обновление 7.7).
- Альт СП Сервер 10.
- Альт Сервер 10.
- Альт 8 СП Сервер (ЛКНВ.11100-01).
- Альт 8 СП Сервер (ЛКНВ.11100-02).
- Альт 8 СП Сервер (ЛКНВ.11100-03).
- Альт СП Рабочая станция 10 64-разрядная.
- Альт Рабочая станция 10 64-разрядная.
- Oracle Linux 9.
- Oracle Linux 8.
- Oracle Linux 7.
- Platform V SberLinux OS Server (SLO) 8.8 64-разрядная.
- РЕД ОС 7.3 Сервер.
- РЕД ОС 7.3 Сертифицированная редакция.
- РЕД ОС 8 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 соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center Web Console.

Браузеры:

- Google™ Chrome™ 125.0.6422.76 или выше (официальная сборка).
- Microsoft Edge 100 или выше.
- Safari® 17.1 для macOS®;
- Яндекс Браузер 24.4.3.1012 и выше.
- Mozilla Firefox Extended Support Release 115.9.1 и выше.

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.

Операционные системы. Рабочие станции Microsoft Windows

- 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, 1709, 1803, 1809 32-разрядная/64-разрядная.
- Microsoft Windows 10 20H2, 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 TH1 (July 2015) Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 RS4 (April 2018 Update, 17134) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 RS5 (October 2018) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 RS6 (May 2019) Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.

- Microsoft Windows 10 20H1 (May 2020 Update) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 20H2 (October 2020 Update) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 21H1 (May 2021 Update) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 21H2 (October 2021 Update) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 10 22H2 (October 2023 Update) Home/Pro/Pro для Workstations/Enterprise/Education 32-разрядная/64-разрядная.
- Microsoft Windows 11 Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 11 22H2 Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 11 23H2 Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 11 24H2 Home/Pro/Pro для Workstations/Enterprise/Education 64-разрядная.
- Microsoft Windows 8.1 Pro/Enterprise 32-разрядная/64-разрядная.
- Microsoft Windows 8 Pro/Enterprise 32-разрядная/64-разрядная.
- Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium Service Pack 1 и выше 32-разрядная/64-разрядная.
- Microsoft Windows XP Professional Service Pack 2 32-разрядная/64-разрядная (поддерживается Агентом администрирования версии 10.5.1781).
- Microsoft Windows XP Professional Service Pack 3 и выше 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32-разрядная (поддерживается Агентом администрирования версии 14.0.0.20023).
- Microsoft Windows Small Business Server 2011 Standard/Essentials 64-разрядная.
- Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-разрядная.
- Microsoft Windows Server 2008 Foundation Service Pack 2 32-разрядная/64-разрядная.
- Microsoft Windows Server 2008 Standard/Enterprise/Datacenter Service Pack 2 32-разрядная/64-разрядная.
- Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Core Mode/Standard Service Pack 1 и выше 64-разрядная.
- Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная.
- Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-разрядная.
- Windows Server 2016 Datacenter/Standard (вариант установки Server Core) (LTSB) 64-разрядная.
- Microsoft Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
- Microsoft Windows Server 2019 RS5 Essentials/Standard 64-разрядная.

- Microsoft Windows Server 2022 Standard/Datacenter/Core 64-разрядная.
- Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-разрядная.

Операционные системы. Linux

- 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) 64-разрядная.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- Ubuntu Server 22.04 LTS ARM 64-разрядная.
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
- CentOS 6.7 and later 32-разрядная.
- CentOS 6.x (до 6.6) 32-разрядная/64-разрядная.
- CentOS 7.x 64-разрядная.
- CentOS Stream 8 64-разрядная.
- CentOS Stream 9 64-разрядная.
- CentOS Stream 9 ARM 64-разрядная.
- Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная.
- Red Hat Enterprise Linux Server 7.x 64-разрядная.
- Red Hat Enterprise Linux Server 8.x 64-разрядная.
- Red Hat Enterprise Linux Server 9.x 64-разрядная.
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) ARM 64-разрядная.
- openSUSE 15 64-разрядная.
- EulerOS 2.0 SP10 64-разрядная.
- EulerOS 2.0 SP10 ARM 64-разрядная.

- Astra Linux Special Edition РУСБ.10015-03 (обновление 7.6) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-37 (обновление 7.7) 64-разрядная.
- Альт Рабочая станция 10.1 64-разрядная.
- Альт Сервер 10.1 64-разрядная.
- ALT Education 10.1 64-разрядная.
- Альт СП Сервер 10 32-разрядная/64-разрядная.
- Альт СП Сервер 10 ARM 64-разрядная.
- Альт СП Рабочая станция 10 32-разрядная/64-разрядная.
- Альт СП Рабочая станция 10 ARM 64-разрядная.
- Альт Сервер 10 64-разрядная.
- Альт Сервер 10 ARM 64-разрядная.
- Альт Рабочая станция 10 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (8.4) ARM 64-разрядная.
- Альт 8 СП Сервер (8.4) ARM 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-03) 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.
- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Oracle Linux 9 64-разрядная.
- Linux Mint 20.x 64-разрядная.
- Linux Mint 21.1 и выше 64-разрядная.
- AlterOS 7.5 или выше 64-разрядная.
- ГосЛинукс IC6/7.17 64-разрядная.
- ГосЛинукс IC6/7.2 64-разрядная.
- SberOS 3.2.0 64-разрядная.

- Platform V SberLinux OS Server (SLO) 8.8 64-разрядная.
- РЕД ОС 7.3 ARM 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- РЕД ОС 8 64-разрядная.
- ROSA Enterprise Linux Server 7.9 64-разрядная.
- ROSA Enterprise Linux Desktop 7.9 64-разрядная.
- РОСА "КОБАЛЬТ" 7.9 64-разрядная.
- РОСА "ХРОМ" 12 64-разрядная.
- AlmaLinux 8 и выше 64-разрядная.
- AlmaLinux 9 и выше 64-разрядная.
- Rocky Linux 8 и выше 64-разрядная.
- Rocky Linux 9 и выше 64-разрядная.
- МСВСфера 9.2 Сервер 64-разрядная.
- МСВСфера 9.2 АРМ 64-разрядная.
- СинтезМ Сервер 8.6 64-разрядная.
- СинтезМ Клиент 8.6 64-разрядная.
- ОСнова 2.10 64-разрядная.
- TeNIX WS 64-разрядная.
- Kylin 10 64-разрядная.
- EMIAS 1.0 64-разрядная.
- Amazon Linux 2 64-разрядная.
- МосОС 15.4 Arbat 64-разрядная.
- Операционная система «Московской электронной школы» 64-разрядная.

Операционные системы. macOS

- macOS Monterey (12.x).
- macOS Ventura (13.x).
- macOS Sonoma (14.x).

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

Платформы виртуализации

- VMware vSphere 8.0.
- 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 Small Business Server 2011 Premium убедитесь, что у вас установлены обновления для Windows: Security Update for Windows 7 (KB3063858) (https://www.microsoft.com/en-us/download/details.aspx?id=47409), Security Update for Windows 7 for x64-based Systems (KB3063858) (https://www.microsoft.com/en-us/download/details.aspx?id=47442), Security Update for Windows Server 2008 (KB3063858) (https://www.microsoft.com/en-us/download/details.aspx?id=47411), Security Update for Windows Server 2008 x64 Edition (KB3063858) (https://www.microsoft.com/en-us/download/details.aspx?id=47414), Security Update for Windows Server 2008 R2 x64 Edition (KB3063858) (https://www.microsoft.com/en-us/download/details.aspx?id=47479).

В Microsoft Windows XP Агент администрирования может не выполнять некоторые операции правильно (см. стр. 239).
Вы можете установить или обновить Агент администрирования для Windows XP только в Microsoft Windows XP. Поддерживаемые редакции Microsoft Windows XP и соответствующие им версии Агента администрирования указаны в списке поддерживаемых операционных систем. Вы можете скачать необходимую версию Агента администрирования для Microsoft Windows XP с этой страницы https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint.
Рекомендуется устанавливать ту же версию Агента администрирования для Linux, что и Kaspersky Security Center.
Kaspersky Security Center полностью поддерживает Агент администрирования той же версии или выше.
Агент администрирования для macOS поставляется вместе с приложением безопасности "Лаборатории Касперского" для этой операционной системы.

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.

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

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

В приложении Kaspersky Security Center реализованы следующие функции безопасности:

- аудит безопасности приложения;
- управление безопасностью;
- сигнализация;
- управление установкой обновлений (актуализации) базы данных признаков вредоносных приложений (вирусов) (БД ПКВ);
- централизованная установка программного обеспечения.

По сравнению с Kaspersky Security Center на базе Windows, Kaspersky Security Center на базе Linux имеет другой набор функций (см. стр. 34).

Приложение 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 приложений "Лаборатории Касперского".
- Выполнять удаленную установку приложений "Лаборатории Касперского" и других приложений сторонних производителей.
- Централизованно распространять лицензионные ключи приложений "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе приложений и устройств.
- Получать уведомления о критических событиях в работе приложений "Лаборатории Касперского".

- Проводить инвентаризацию оборудования, подключенного к сети организации.
- Централизованно работать с файлами, помещенными приложениями безопасности на карантин или в резервное хранилище, а также с файлами, обработка которых отложена приложениями безопасности.

В этом разделе

Совместимые приложения и решения "Лаборатории Касперского"

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

- Kaspersky Endpoint Security для Windows 12.0 и выше (поддерживает файловые серверы).
- Kaspersky Endpoint Security для Linux 11.2 и выше (поддерживает файловые серверы).
- Kaspersky Endpoint Security для Linux Elbrus Edition 10 и выше.
- Kaspersky Endpoint Security для Linux ARM Edition 11.2 и выше.
- Kaspersky Endpoint Security для Mac 11.3 и выше.
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 и выше.
- Kaspersky Industrial CyberSecurity for Nodes 3.2 и выше.
- Kaspersky Industrial CyberSecurity for Networks 3.2 и выше.
- Kaspersky Endpoint Agent 3.15 и выше.
- Kaspersky Embedded Systems Security для Windows 3.2 и выше.
- Kaspersky Embedded Systems Security для Linux 3.3 и выше.
- Kaspersky Security для виртуальных сред Легкий агент 5.2 и выше.

Kaspersky Security Center входит в состав следующих решений:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response

Подробнее о версиях приложений и решений см. на странице "Жизненный цикл приложений" https://support.kaspersky.com/corporate/lifecycle.

Список ограничений

Kaspersky Security Center поддерживает управление Kaspersky Endpoint Security для Windows со следующими ограничениями: компонент Kaspersky Sandbox не поддерживается.

Единый вход (SSO) не поддерживается для Kaspersky Industrial CyberSecurity for Networks.

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 установленного приложения Kaspersky Security Center Web Console совместима с версией Сервера администрирования, к которому вы подключаетесь:

- Web Console, включенное в приложение Kaspersky Security Center 15.1, поддерживает Сервер администрирования Kaspersky Security Center следующих версий: 15 и 14.2.
- Сервер администрирования, включенный в приложение Kaspersky Security Center 15.1, поддерживает Kaspersky Security Center Web Console следующих версий: 15 и 14.2.

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

"Лаборатории Касперского" предлагает приложение Kaspersky Security Center в качестве локального решения для двух платформ – Windows и Linux. В решении для Windows вы устанавливаете Сервер администрирования на устройство с операционной системой Windows. Решение на базе Linux имеет версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Эта справка содержит информацию о Kaspersky Security Center. Для получения подробной информации о решении на базе Windows см. справку Kaspersky Security Center Windows https://support.kaspersky.com/KSC/14.2/ru-RU/5022.htm.

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

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

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Расположение Сервера администрирования	Локально	Локально
Расположение системы управления базами данных (СУБД)	Локально	Локально

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Операционная система для установки Сервера администрирования	Windows	Linux
Тип Консоли администрирования	Локальная и веб-интерфейс	Веб-интерфейс
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Linux
Иерархия Серверов администрирования	✓	✓
Иерархия групп администрирования	✓	✓
Опрос сети	✓	✓
Максимальное количество управляемых устройств	100 000	50 000 (с PostgreSQL и Postgres Pro)
Защита устройств под управлением Windows, macOS и Linux	✓	✓
Защита мобильных устройств	✓	—
Защита виртуальных машин	✓	✓
Защита публичной облачной инфраструктуры	✓	—
Управление безопасностью, ориентированное на устройства (см. стр. 394)	✓	✓
Управление безопасностью, ориентированное на пользователя (см. стр. 394)	✓	✓

kaspersky

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Политики приложений	✓	✓
Задачи для приложений "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	✓
Прокси-сервер KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Централизованное распространение лицензионных ключей приложений "Лаборатории Касперского"	✓	✓
Автоматическое обновление антивирусных баз	✓	✓
Поддержка виртуальных Серверов администрирования	✓	✓
Установка обновлений приложений сторонних производителей и поиск уязвимостей в приложениях сторонних производителей	✓	✓
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
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 Kaspersky Security Center	✓	✓
Установка Сервера администрирования на отказоустойчивом кластере Windows Server	✓	—
Использование SNMP для отправки статистики Сервера администрирования приложениям сторонних производителей	✓	—
Удаленная диагностика клиентских устройств	✓	✓
Удаленное подключение к рабочему столу клиентского устройства	✓	—
Работа с ревизиями объектов	✓	✓

Функция или свойство	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Автоматическое обновление приложений "Лаборатории Касперского"	✓	✓
Развертывание операционных систем на клиентских устройствах	✓	—
Веб-сервер для публикации инсталляционных пакетов и других файлов	✓	✓
Просмотр и работа с алертами, зарегистрированными Endpoint Detection and Response	✓	✓
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	✓	✓
Управление сторонними лицензиями	✓	—

kaspersky

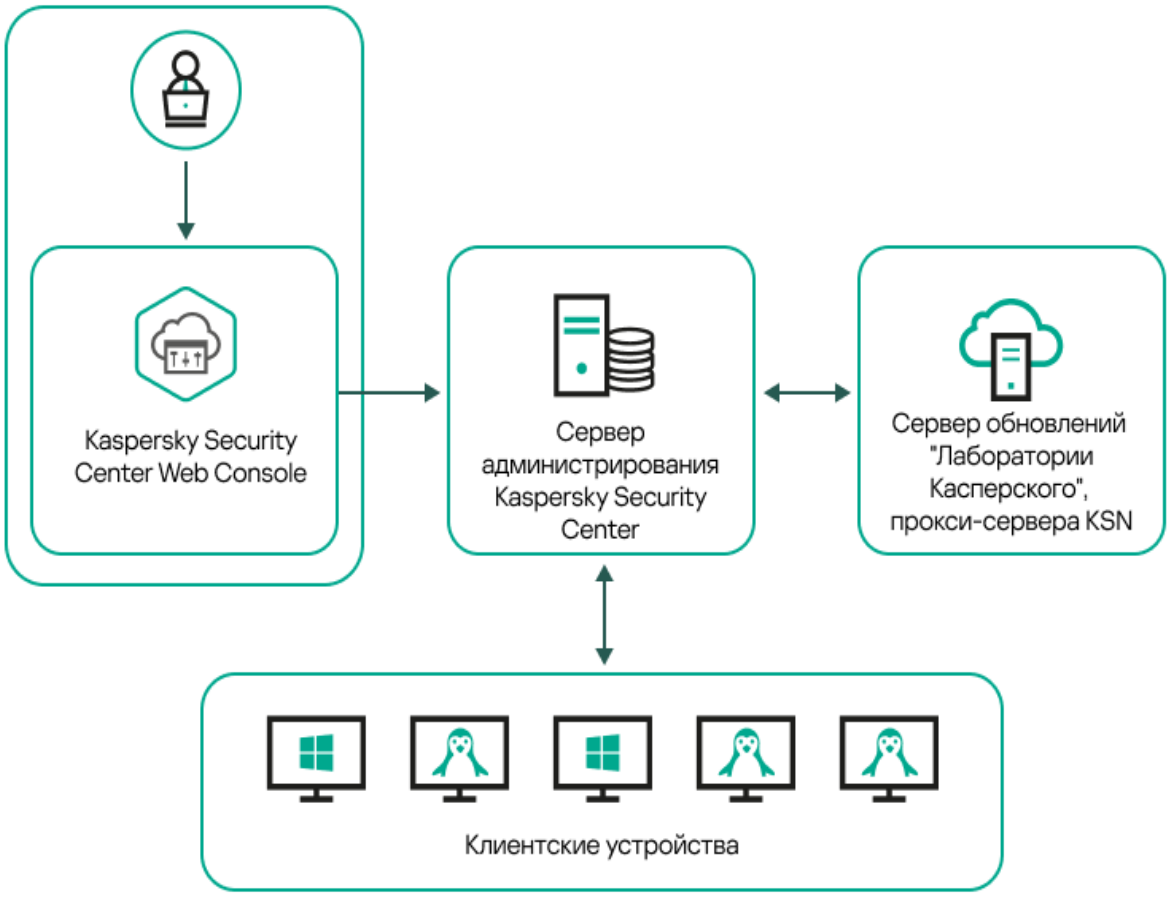
Архитектура и основные понятия

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

В этом разделе

Архитектура приложения

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 приложениях и управления ими.
- **Серверы обновлений "Лаборатории Касперского"**. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.
- **Серверы KSN**. Серверы содержат оперативную базу знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network (см. стр. 445) обеспечивает более высокую скорость реакции приложений "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

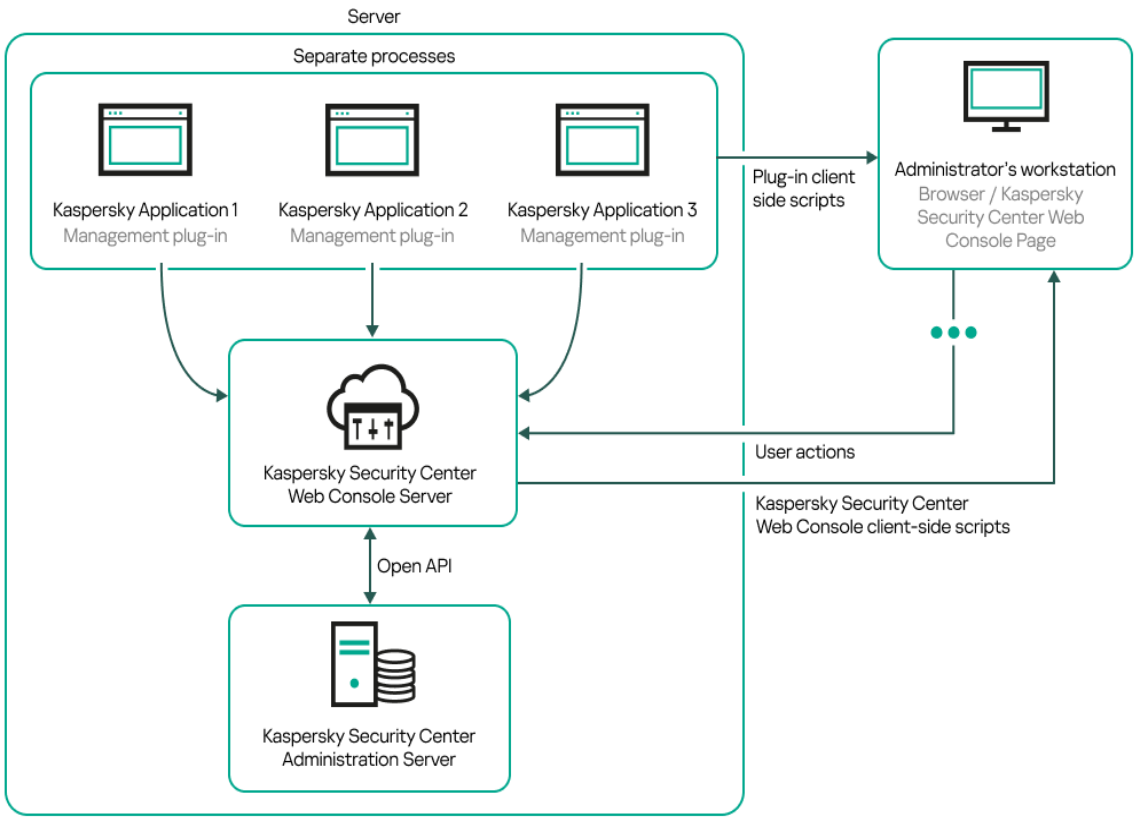
- **Клиентские устройства.** Клиентские устройства организации защищены Kaspersky Security Center. На каждом защищаемом устройстве должно быть установлено одно из приложений безопасности "Лаборатории Касперского".

См. также:

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения.....77

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 приложениями "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждого приложения), 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. 93). Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования (см. стр. 177).

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
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. 425).
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. 177).
14000	klserver	TCP	Прием подключений от Агентов администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию при настройке портов подключения (см. стр. 93) при установке Kaspersky Security Center или при подключении клиентского устройства к Серверу администрирования вручную (см. стр. 137).
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. 446).

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
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. 446).
17000	klactprx	TCP (TLS)	Прием подключений для активации приложений 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. 173)	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, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MariaDB). 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. 104). 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 распространения к Агентам администрирования	Управление клиентскими устройствами. Вы можете изменить значения портов по умолчанию в окне свойств политики Агента администрирования (см. стр. 425).
15000	klnagent	Широковещательная рассылка UDP	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. 290).

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. 290)	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов. Вы можете изменить значения портов по умолчанию в свойствах точки распространения (см. стр. 290).
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. 290).
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. 290).

kaspersky

См. также:

Порты, используемые приложением 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 приложением 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 KSCWebConsoleManagementService, 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 приложения Kaspersky Security Center Web Console.

Номер порта	Имя службы	Протокол	Назначение порта	Область
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.....42

kaspersky

Основные понятия

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

В этом разделе

Сервер администрирования

Компоненты Kaspersky Security Center позволяют осуществлять удаленное управление приложениями "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:

- с именем `kladminserver_srv;`
- с автоматическим типом запуска при старте операционной системы;
- с учетной записью `ksc` либо учетной записью пользователя в соответствии с выбором, сделанным при установке Сервера администрирования.

Полный список параметров установки см. в разделе: Установка Kaspersky Security Center (см. стр. 93).

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов приложений;
- удаленная установка приложений на клиентские устройства и удаление приложений;
- обновление баз и модулей приложений "Лаборатории Касперского";
- управление политиками и задачами на клиентских устройствах;
- хранение информации о событиях, произошедших на клиентских устройствах;
- формирование отчетов о работе приложений "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 приложения

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 приложение Kaspersky Security Center Web Console, установленное на устройство под управлением Linux, то приложение отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов (см. стр. 106).

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

См. также:

Начало работы 87

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Иерархия Серверов администрирования

Серверы администрирования могут образовывать 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. 52).

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:

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования 82

Начало работы 87

ВВиртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент приложения Kaspersky Security Center, предназначенный для управления антивирусной защитой 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).

Кроме того, виртуальный Сервер администрирования имеет следующие ограничения:

- В окне свойств виртуального Сервера ограничен набор разделов.
- Для удаленной установки приложений "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.
- Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

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 приложения безопасности 239

группы администрирования.

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

Для всех управляемых устройств в группе администрирования устанавливаются:

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

Управляемое 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 управляемые 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, устройство будут автоматически переданы параметры приложений, необходимые для 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 приложений, 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 273
Сценарий: настройка защиты сети.....393

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 приложения.

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

Рабочее место администратора

Устройства, на которых установлен Сервер Kaspersky Security Center Web Console, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление приложениями "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 приложениями "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 определенным приложением "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для приложения.

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. 452) и параметров приложения.

- Интерфейс для создания и изменения политик и профилей политик (см. стр. 400) для удаленной централизованной настройки приложений "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных приложениями.
- Функции Kaspersky Security Center Web Console для отображения оперативных данных и событий приложения, а также статистики, полученной от клиентских устройств.

См. также:

Совместимые приложения и решения "Лаборатории Касперского" 33

Развертывание приложений "Лаборатории Касперского".....333

Политики

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 55) и ее подгруппам. Вы можете установить несколько приложений "Лаборатории Касперского" (см. стр. 33) на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "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 приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "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 одного приложения можно настроить несколько политик с различными значениями.
- Для одного приложения 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 локального приложения, 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.

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 400
Создание профиля политики 420

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 приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

kaspersky

Вы можете создать задачу для приложения, только если для этого приложения 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 приложения 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 каждого приложения 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 запущено приложение, для которого 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. 589).

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

См. также:

Начало работы 87

Область действия задачи

Область задачи (см. стр. 452) – 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 для выборок устройств 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 приложения

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

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

Значение параметра, которое использует приложение 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 приложение использует локальное значение параметра, а не то, которое указано в политике. При этом значение параметра может изменяться через локальные параметры приложения.

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

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

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

См. также:

Политики и профили политик 400

Точка распространения

Точка распространения (ранее называлась «агент обновлений») – это устройство с установленным Агентом администрирования, который используется для распространения обновлений, удаленной установки приложений, 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 приложений "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. 290). В этом случае на устройстве запустится служба прокси-сервера KSN (см. стр. 450).

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 невозможно 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 приложения, 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 285

kaspersky

Схемы трафика данных и использования портов

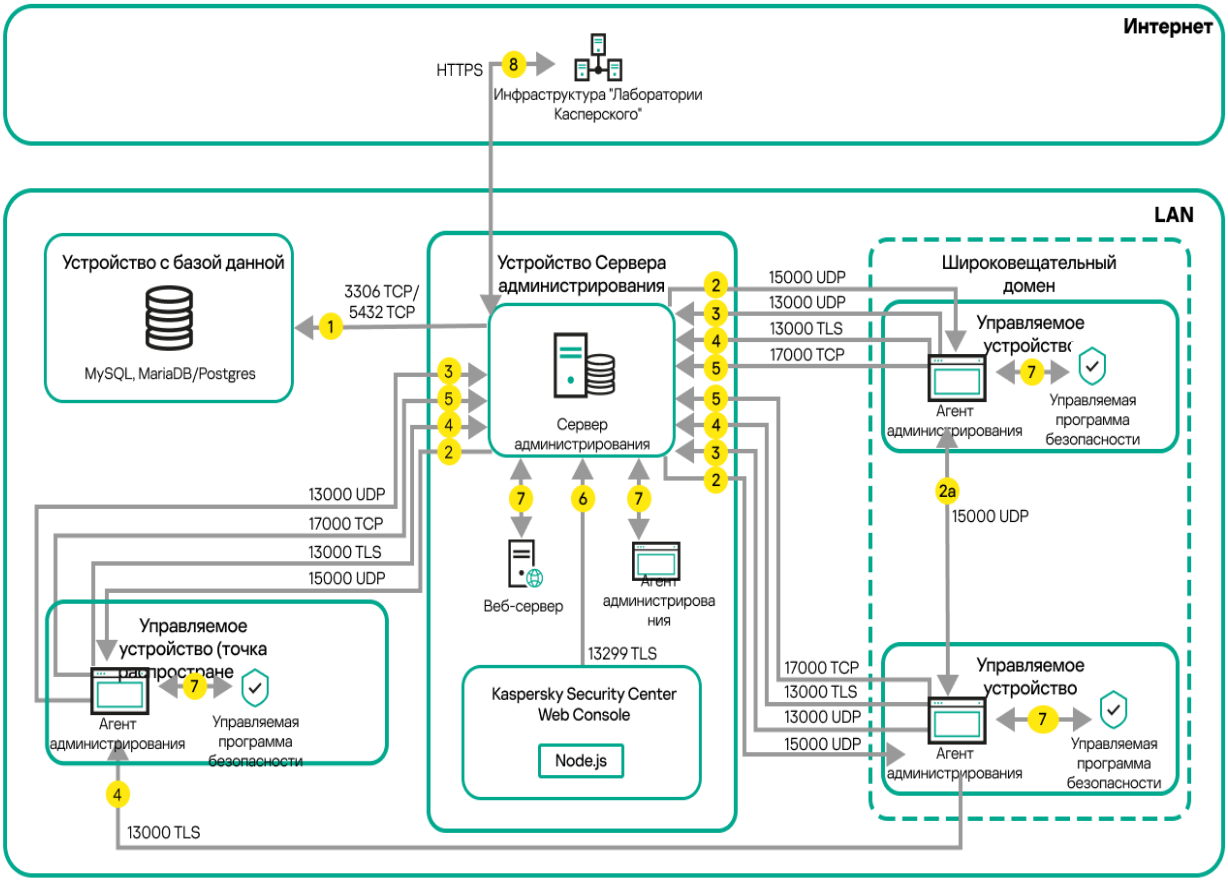
В этом разделе приведены схемы трафика данных между компонентами Kaspersky Security Center, управляемыми приложениями безопасности и внешними серверами для различных конфигураций. Схемы содержат номера портов, которые должны быть доступны на локальных устройствах.

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. 234). Если количество управляемых устройств мало, все управляемые устройства могут получать обновления непосредственно с Сервера администрирования.

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

1. Сервер администрирования передает данные в базу данных (см. стр. 79). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно 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 (см. стр. 80).

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 с Сервером администрирования на эти устройства не отправляются напрямую.

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 (см. стр. 80) и от подчиненных Серверов администрирования (см. стр. 82) 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.
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. Приложения 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 приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

См. также:

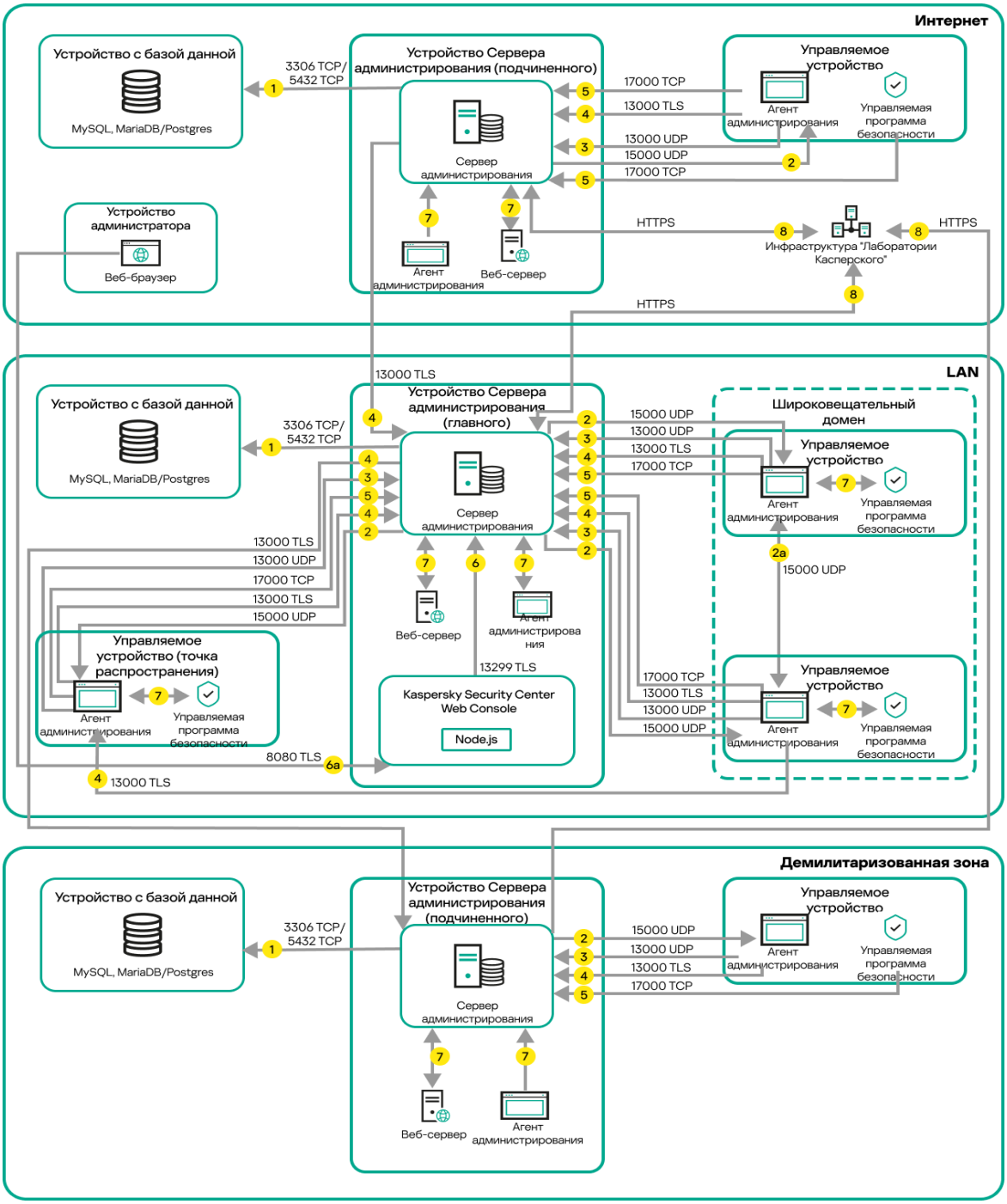
Типовая конфигурация: один офис 228

Порты, используемые Kaspersky Security Center 42

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

На рисунке показана иерархия Серверов администрирования: главный Сервер администрирования расположен внутри локальной сети (LAN). Подчиненный Сервер администрирования находится в

демилитаризованной зоне (DMZ); другой подчиненный Сервер администрирования расположен в интернете.



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

1. Сервер администрирования передает данные в базу данных (см. стр. 79). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно 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 (см. стр. 80).

   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 с Сервером администрирования на эти устройства не отправляются напрямую.

3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.

4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 80) и от подчиненных Серверов администрирования (см. стр. 82) 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.

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 (см. стр. 86). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

7. Приложения 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 приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

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

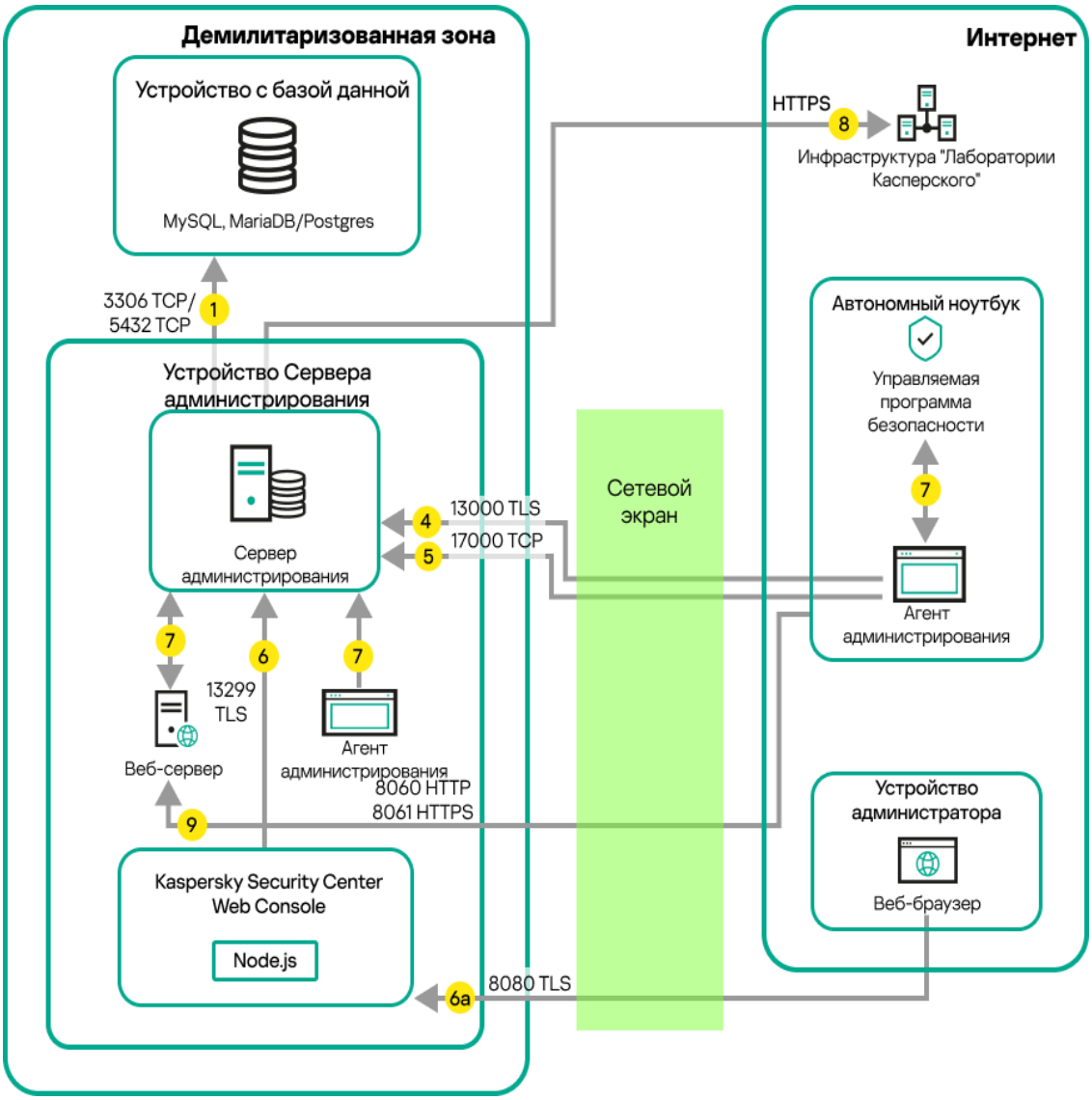
См. также:

Иерархия Серверов администрирования 177

Порты, используемые Kaspersky Security Center 42

Сервер администрирования внутри локальной сети (LAN), управляемые устройства в интернете; использование сетевого экрана

На рисунке ниже показан трафик данных, когда Сервер администрирования находится внутри локальной сети (LAN), а управляемые устройства находятся в интернете. На этом рисунке используется выбранный вами корпоративный сетевой экран. Дополнительную информацию см. в документации к приложению.



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

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

1. Сервер администрирования передает данные в базу данных (см. стр. 79). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно 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 (см. стр. 80).

   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 с Сервером администрирования на эти устройства не отправляются напрямую.
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 80) и от подчиненных Серверов администрирования (см. стр. 82) 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.
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 (см. стр. 86). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
7. Приложения 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 приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.
9. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 53), который находится на том же устройстве, на котором установлен Сервер администрирования.

kaspersky

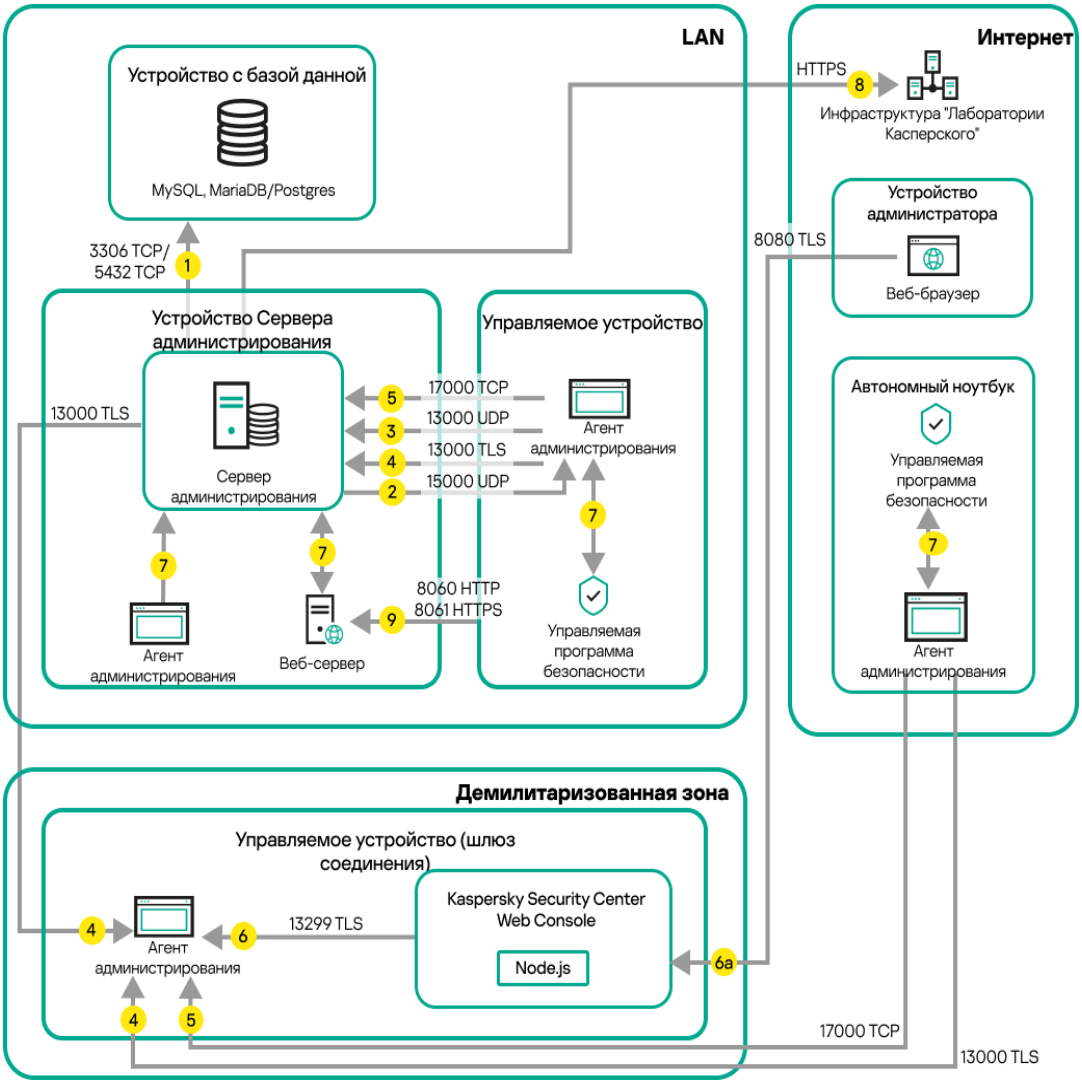
См. также:

Порты, используемые Kaspersky Security Center.....42

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 (см. стр. 79). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно 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 (см. стр. 80).

   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 с Сервером администрирования на эти устройства не отправляются напрямую.
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 80) и от подчиненных Серверов администрирования (см. стр. 82) 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.
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 (см. стр. 86). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.
7. Приложения 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 приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

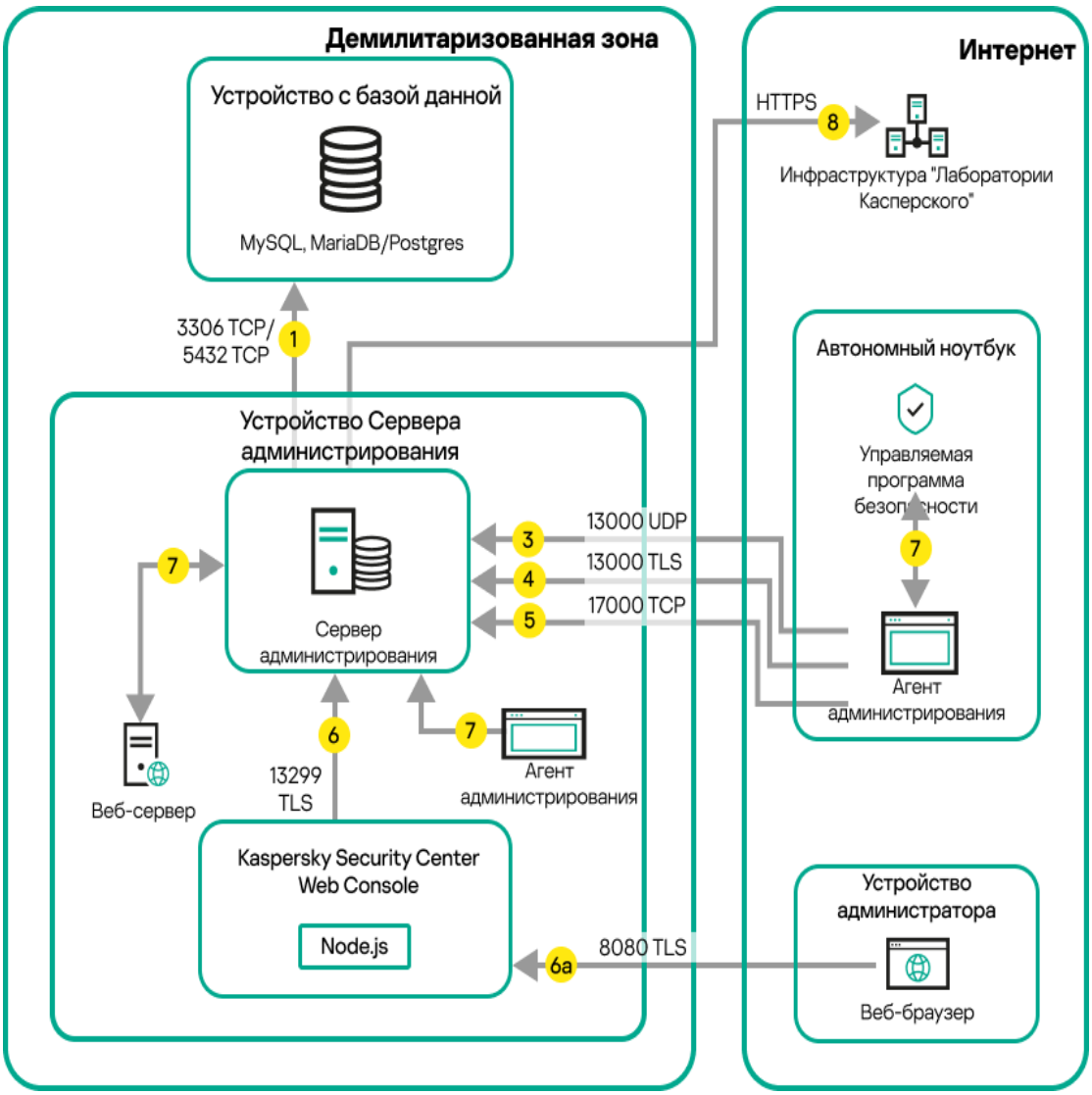
   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно управлять этими данными вручную.

9. Запросы на пакеты от управляемых устройств, включая мобильные устройства, передаются на Веб-сервер (см. стр. 53), который находится на том же устройстве, на котором установлен Сервер администрирования.

См. также:

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 (см. стр. 79). Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно 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 (см. стр. 80).

   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 с Сервером администрирования на эти устройства не отправляются напрямую.
3. Информация о выключении управляемых устройств передается от Агента администрирования на Сервер администрирования через UDP-порт 13000.
4. Сервер администрирования принимает подключения от Агентов администрирования (см. стр. 80) и от подчиненных Серверов администрирования (см. стр. 82) 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.

   4a. Шлюз соединений в демилитаризованной зоне (см. стр. 63) также принимает подключение от Сервера администрирования по SSL-порту 13000 (см. стр. 85). Так как шлюз соединения в демилитаризованной зоне не может получить доступ к портам Сервера администрирования, Сервер администрирования создает и поддерживает постоянное сигнальное соединение со шлюзом соединения. Сигнальное соединение не используется для передачи данных; оно используется только для отправки приглашения к сетевому взаимодействию. Когда шлюзу соединения необходимо подключиться к Серверу, он уведомляет Сервер через это сигнальное соединение, а затем Сервер создает необходимое соединение для передачи данных.

   Внешние устройства также подключаются к шлюзу соединения через SSL-порт 13000 (см. стр. 85).
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 (см. стр. 86). Сервер Kaspersky Security Center Web Console можно установить на то же устройство, на котором установлен Сервер администрирования, или на другое устройство.

7. Приложения 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 приложений и обновления антивирусных баз) передаются по протоколу HTTPS.

   Если вы не хотите иметь доступ в интернет на вашем Сервере администрирования, вам нужно 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. 53).

См. также:

Порты, используемые Kaspersky Security Center 42

Доступ из интернета: Сервер администрирования в демилитаризованной зоне 231

kaspersky

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения

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

В этом разделе

См. также:

Условные обозначения в схемах взаимодействия

В таблице ниже приведены условные обозначения, использованные в схемах.

Таблица 8. Условные обозначения

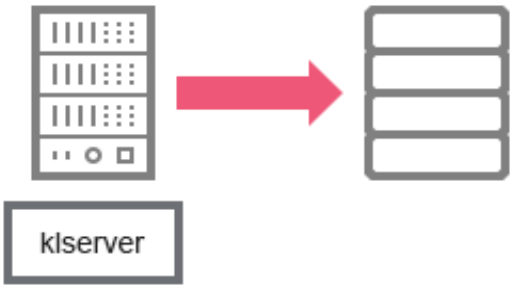
Иконка	Значение
	Сервер администрирования

Иконка	Значение
	Подчиненный Сервер администрирования
	СУБД
	Клиентское устройство, на котором установлены Агент администрирования и приложение семейства Kaspersky Endpoint Security (либо другое приложение безопасности, которым может управлять Kaspersky Security Center)
	Шлюз соединения
	Точка распространения
	Браузер на устройстве пользователя
	Процесс, запущенный на устройстве и открывающий какой-либо порт
	Порт и его номер
	Трафик TCP (направление стрелки обозначает направление трафика)
	Трафик UDP (направление стрелки обозначает направление трафика)
	Транспорт СУБД

Иконка	Значение
	Границы демилитаризованной зоны

Сервер администрирования и СУБД

Данные от Сервера администрирования попадают в базу данных (см. стр. 229).



Если вы установили Сервер администрирования и базу данных на разные устройства, вам нужно сделать доступными необходимые порты на устройстве, где расположена база данных (например, порт 3306 для MariaDB). Подробную информацию см. в документации СУБД.

См. также:

Условные обозначения в схемах взаимодействия 77

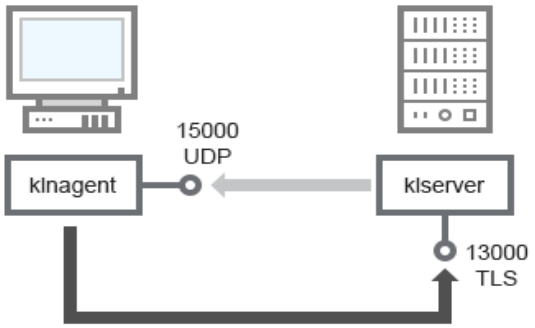
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

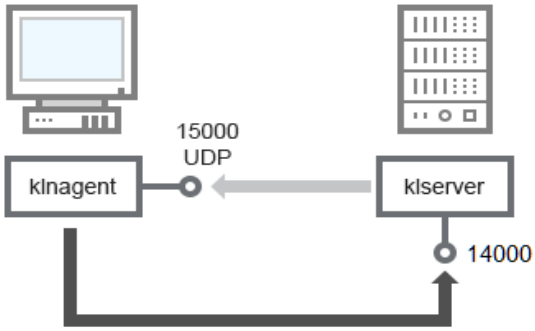
kaspersky

Сервер администрирования и клиентское устройство: Управление приложением безопасности

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



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



Пояснения к схемам см. в таблице ниже.

Таблица 9. Сервер администрирования и клиентское устройство: управление приложением безопасности (трафик)

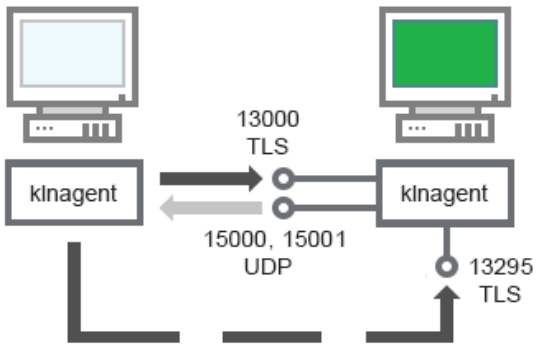
Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта
Агент администрирования	15000	klnagent	UDP	Многоадресная рассылка Агентам администрирования
Сервер администрирования	13000	klserver	TCP (TLS)	Прием подключений от Агентов администрирования
Сервер администрирования	14000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

kaspersky

См. также:

Обновление программного обеспечения на клиентском устройстве с помощью точки распространения

Клиентское устройство подключается к точке распространения через порт 13000 и, если вы используете точку распространения в качестве push-сервера (см. стр. 295), также через порт 13295; точка распространения выполняет многоадресную рассылку Агентам администрирования через порт 15000 (см. рисунок ниже). Обновления и инсталляционные пакеты поступают с точки распространения через порт 15001.



Пояснения к схеме см. в таблице ниже.

Таблица 10. Обновление программного обеспечения с помощью точки распространения (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта
Агент администрирования	15000	klnagent	UDP	Многоадресная рассылка Агентам администрирования
Агент администрирования	15001	klnagent	UDP	Получение обновлений и инсталляционных пакетов от точки распространения
Точка распространения	13000	klnagent	TCP (TLS)	Прием подключений от Агентов администрирования
Точка распространения	13295	klnagent	TCP (TLS)	Получение подключений от клиентских устройств (push-сервера)

См. также:

Условные обозначения в схемах взаимодействия 77

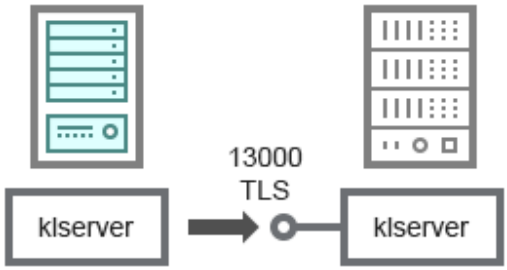
Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования

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

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Kaspersky Security Center Web Console, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13299 главного Сервера был доступен.



Пояснения к схеме см. в таблице ниже.

Таблица 11. Иерархия Серверов администрирования (трафик)

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

См. также:

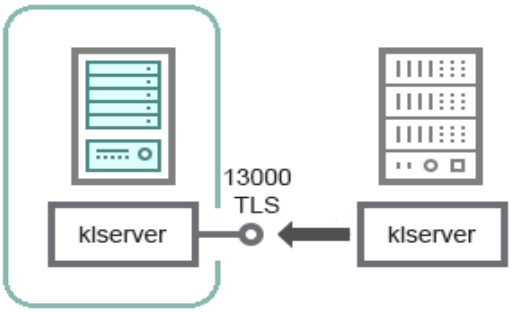
Условные обозначения в схемах взаимодействия 77

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

kaspersky

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне



На схеме показана иерархия Серверов администрирования, в которой подчиненный Сервер, находящийся в демилитаризованной зоне, принимает подключение от главного Сервера (пояснения к схеме см. в таблице ниже). При объединении Серверов в иерархию необходимо, чтобы порт 13299 обоих Серверов был доступен. Приложение Kaspersky Security Center Web Console подключается к Серверу администрирования по порту 13299.

В дальнейшем, после объединения Серверов в иерархию, вы сможете администрировать оба Сервера через Kaspersky Security Center Web Console, подключенную к главному Серверу администрирования. Таким образом, необходимо только, чтобы порт 13299 главного Сервера был доступен.

Таблица 12. Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне (трафик)

Устройство	Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта
Подчиненный Сервер администрирования	13000	klserver	TCP (TLS)	Прием подключений от главного Сервера администрирования

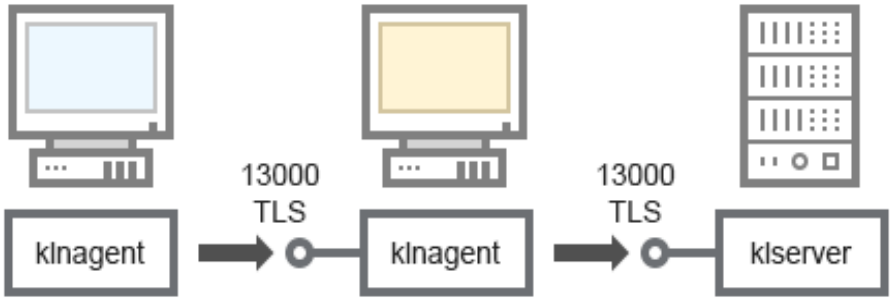
См. также:

Условные обозначения в схемах взаимодействия 77

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство



Пояснения к схеме см. в таблице ниже.

Таблица 13. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

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

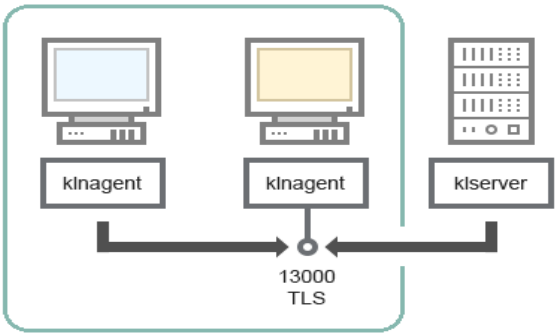
См. также:

Условные обозначения в схемах взаимодействия 77

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

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



Пояснения к схеме см. в таблице ниже.

Таблица 14. Сервер администрирования, шлюз соединений в сегменте сети и клиентское устройство (трафик)

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

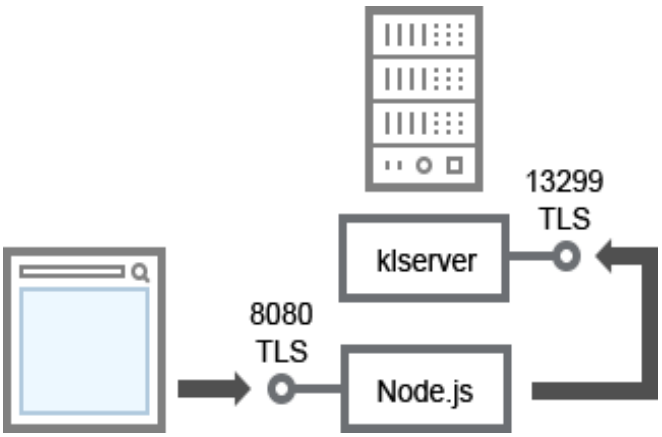
См. также:

Условные обозначения в схемах взаимодействия 77

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

Сервер администрирования и Kaspersky Security Center Web Console



Пояснения к схеме см. в таблице ниже.

Таблица 15. Сервер администрирования и Kaspersky Security Center Web Console (трафик)

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

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

См. также:

Условные обозначения в схемах взаимодействия 77

Взаимодействие компонентов Kaspersky Security Center и приложений безопасности: дополнительные сведения 77

Порты, используемые Kaspersky Security Center 42

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 приложения "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 приложений безопасности "Лаборатории Касперского".

Если вы хотите попробовать Kaspersky Security Center, вы можете получить пробную тридцатидневную версию на веб-сайте "Лаборатории Касперского" https://www.kaspersky.ru/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. 40). 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. 224).

   Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования (см. стр. 51). 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. 129) и убедитесь, что они соответствуют всем требованиям (см. стр. 131).

3. **Установка системы управления базами данных (СУБД)**

   Установите СУБД, используемую Kaspersky Security Center, или используйте существующую СУБД.

   Вы можете выбрать одну из поддерживаемых (см. стр. 22) версий MariaDB. Сведения о том, как установить выбранную СУБД, см. в документации к ней.

   Если дистрибутив вашей операционной системы на базе Linux не содержит поддерживаемую СУБД, вы можете установить СУБД из стороннего хранилища пакетов. Если установка дистрибутивов из сторонних хранилищ запрещена, вы можете установить СУБД на отдельном устройстве.

   > 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. 91), PostgreSQL (см. стр. 93) или Postgres Pro (см. стр. 93) используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

Если вы хотите изменить тип СУБД после установки (см. стр. 124), вам необходимо переустановить Kaspersky Security Center. Данные могут быть частично и вручную перенесены в другую базу данных.

4. **Настройка портов**

   Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты открыты необходимые порты (см. стр. 42).

   Если требуется предоставить доступ к Серверу администрирования из интернета (см. стр. 230), настройте порты и параметры подключения в зависимости от конфигурации сети.

5. **Установка компонентов 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. 22), и установите на устройство Kaspersky Security Center (см. стр. 93). 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. 22), 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 установлено приложение Kaspersky Security Center Web Console.

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

   По умолчанию приложение 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. 143). Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики (см. стр. 400) и задачи (см. стр. 452) с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач (см. стр. 393).

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 приложения

"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. 281) с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам (см. стр. 276) 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. 233). 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 приложений безопасности на устройства в сети**

    Развертывание защиты в сети организации подразумевает установку Агента администрирования и приложений безопасности на устройства (см. стр. 333), найденные Сервером администрирования в процессе обнаружения устройств.

    Чтобы выполнить удаленную установку приложения, запустите мастер развертывания защиты.

    Приложения безопасности защищают устройства от вирусов и других приложений, представляющих угрозу. Агент администрирования обеспечивает связь устройства с Сервером администрирования. Параметры Агента администрирования автоматически настраиваются по умолчанию.

    Перед тем как установить Агент администрирования и приложения безопасности на устройства в сети, убедитесь, что эти устройства доступны (включены).

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

    Распространите лицензионные ключи (см. стр. 378) на клиентские устройства, чтобы активировать управляемые приложения безопасности на этих устройствах.

14. **Настройка политик приложений "Лаборатории Касперского"**

    Чтобы на различных устройствах были применены разные параметры приложений, можно использовать управление безопасностью устройств или управление безопасностью, ориентированное на пользователей. Управление безопасностью устройств реализуется с помощью политик (см. стр. 400) и задач (см. стр. 452). Задачи могут выполняться только на устройствах, которые соответствуют определенным условиям. Для создания условий отбора устройств используются выборки устройств (см. стр. 304) и теги (см. стр. 318).

15. **Мониторинг состояния защиты сети**

    Вы можете организовывать мониторинг сети с помощью веб-виджетов на информационной панели (см. стр. 551), формировать отчеты (см. стр. 556) о приложениях "Лаборатории Касперского", настраивать и просматривать выборки событий (см. стр. 589), полученные от приложений на управляемых устройствах, и просматривать список уведомлений.

kaspersky

В этом разделе

kaspersky

Установка

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

В этом разделе

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center

Рекомендуемые параметры для файла my.cnf

Подробнее о настройке СУБД см. также в процедуре настройки учетной записи (см. стр. 125). Для получения информации об установке СУБД обратитесь к процедуре установки СУБД (см. стр. 87).

► *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.

Для MariaDB 10.6 дополнительно введите в раздел [mysqld] следующие строки:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

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`, то 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/<ВЕРСИЯ>/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 в 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. 127).

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

Установка компонентов Kaspersky Security Center

В этом разделе описана установка Kaspersky Security Center.

Перед установкой:

- Установите СУБД.
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 22).

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

Чтобы установить Kaspersky Security Center, выполните команды, указанные в инструкции ниже, под учетной записью с привилегиями root.

► *Чтобы установить Kaspersky Security Center:*

1. Если ваше устройство работает под управлением Astra Linux 1.8 или выше, выполните действия, описанные в этом шаге. Если ваше устройство работает под управлением другой операционной системы, переходите к следующему шагу.

   a. Создайте директорию /etc/systemd/system/kladminserver_srv.service.d и файл с именем override.conf со следующим содержимым:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Создайте директорию /etc/systemd/system/klwebsrv_srv.service.d и файл с именем override.conf со следующим содержимым:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

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. 368) 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 256 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:

- Установите систему управления базами данных (СУБД).
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 22).

Чтобы установить Kaspersky Security Center в тихом режиме:

1. Прочитайте Лицензионное соглашение (см. стр. 368). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
2. Если ваше устройство работает под управлением Astra Linux 1.8 или выше, выполните действия, описанные в этом шаге. Если ваше устройство работает под управлением другой операционной системы, переходите к следующему шагу.
   a. Создайте директорию /etc/systemd/system/kladminserver_srv.service.d и файл с именем override.conf со следующим содержимым:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Создайте директорию /etc/systemd/system/klwebsrv_srv.service.d и файл с именем override.conf со следующим содержимым:

```
[Service]
User=
User=ksc
CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
ExecStart=
ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
```

3. 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
```

4. 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.
5. 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
   ```

6. 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`
7. 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 16. 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

Имя переменной	Обязательная	Описание	Возможные значения
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

Имя переменной	Обязательная	Описание	Возможные значения
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

Имя переменной	Обязательная	Описание	Возможные значения
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. 112), 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 KLFOC_UNATT_CONN_MODE имеет значение VirtualAdapter, файл ответов должен включать следующие дополнительные переменные:

Имя переменной	Обязательная	Описание	Возможные значения
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

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:

- Установите СУБД.
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux (см. стр. 22).
- Загрузите ключ приложения 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 пакет совместимости:

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

3. Создайте директорию для ключа приложения:

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

4. Поместите ключ приложения 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. Если ваше устройство работает под управлением Astra Linux 1.8 или выше, выполните действия, описанные в этом шаге. Если ваше устройство работает под управлением другой операционной системы, переходите к следующему шагу.

   a. Создайте директорию /etc/systemd/system/kladminserver_srv.service.d и файл с именем override.conf со следующим содержимым:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Создайте директорию /etc/systemd/system/klwebsrv_srv.service.d и файл с именем override.conf со следующим содержимым:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

7. 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
```

8. Запустите установку Kaspersky Security Center:

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

9. Запустите настройку Kaspersky Security Center:

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

10. Прочитайте Лицензионное соглашения (см. стр. 368) 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.

11. 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 256.
- 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 и Сервер администрирования Kaspersky Security Center (см. стр. 93).

Если вы устанавливаете Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды, следуйте инструкциям для Astra Linux (см. стр. 109).

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 приложение.
3. Создайте файл ответов (см. стр. 106), 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 ALT Linux необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

Приложение Kaspersky Security Center Web Console не может быть обновлено с помощью того же установочного файла .rpm. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки приложения, вам нужно сначала удалить приложение, а затем установить его 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. 139).

kaspersky

Параметры установки Kaspersky Security Center Web Console

Для установки Сервера Kaspersky Security Center Web Console на устройства с операционными системами Linux (см. стр. 104) 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 17. 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 приложением 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. 368). 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. 368). • false – Я не принимаю условия Лицензионного соглашения (выбрано по умолчанию). Если значение не указано, приложение 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. 42).	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. 42).	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%.

Параметр	Описание	Доступные значения
`serviceWebConsoleAccount`	Учетная запись, от имени которой работает служба KSCSvcWebConsole (см. стр. 42).	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. 42).	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%`.
`messageQueueAccount`	Учетная запись, от имени которой работает служба KSCWebConsoleMessageQueue (см. стр. 42).	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 42

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 и Сервер администрирования Kaspersky Security Center (см. стр. 93).

kaspersky

► *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 приложение.
3. Создайте файл ответов (см. стр. 106), 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
   }
   ```

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 пакет совместимости:

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

6. Создайте директорию для ключа приложения:

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

7. Поместите ключ приложения 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. 139).

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

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 Kaspersky Security Center или Microsoft. Перед установкой Kaspersky Security Center Web Console установите СУБД и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center (см. стр. 120).

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

1. Выполните шаг 1 и шаг 2 из раздела Установка Kaspersky Security Center Web Console (см. стр. 104).
2. На шаге 3 в файле ответов (см. стр. 106), укажите `доверенный` параметр установки, разрешающий отказоустойчивому кластеру Kaspersky Security Center 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 Kaspersky Security Center (см. стр. 118). 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 Kaspersky Security Center (см. стр. 117). 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 Kaspersky Security Center, 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. 139).

Вы можете перейти в раздел **Обнаружение устройств и развертывание → Нераспределенные устройства**, чтобы просмотреть информацию об узлах кластера и о файловом сервере (см. стр. 117).

Установка и удаление Агента администрирования, на устройстве с операционной системой TeNIX WS

Установка и удаление Агента администрирования выполняется локально на устройстве.

► *Чтобы установить Агент администрирования на устройство с операционной системой TeNIX WS:*

1. Распакуйте архив с установочным пакетом Агента администрирования в выбранную вами директорию на устройстве.
2. Выполните следующую команду в терминале командной строки:

   ```
   PKGDIR=<директория с установочным пакетом> tpkg klnagent.
   ```

3. Выполните первоначальную настройку Агента администрирования.

► *Чтобы удалить Агент администрирования с устройства с операционной системой TeNIX WS, выполните команду в терминале командной строки:*

```
PKGDIR=<директория с пакетами> tpkg -d klnagent.
```

Развертывание отказоустойчивого кластера Kaspersky Security Center

Этот раздел содержит общую информацию об отказоустойчивом кластере Kaspersky Security Center, а также инструкции по подготовке и развертыванию отказоустойчивого кластера Kaspersky Security Center в вашей сети.

kaspersky

В этом разделе

Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center 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. 114).

Развертывание приложений "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:

   1. Создайте группу с именем "kladmins" и назначьте один и тот же GID всем трем группам.
   2. Создайте учетную запись с именем "ksc" и назначьте один и тот же UID всем трем учетным записям пользователей. Для созданных учетных записей укажите в качестве основной группы kladmins.
   3. Создайте учетную запись с именем "rightless" и назначьте один и тот же UID всем трем учетным записям пользователей. Для созданных учетных записей укажите в качестве основной группы kladmins.

a. Подготовка файлового сервера

Подготовьте файловый сервер к работе в составе отказоустойчивого кластера Kaspersky Security Center. 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 Kaspersky Security Center (см. стр. 117).

b. 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 Kaspersky Security Center (см. стр.118).

c. **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. 22).

d. **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. 111).

e. **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 Kaspersky Security Center развернут. Пожалуйста, ознакомьтесь с событиями, которые приводят к переключению между активными и пассивными узлами (см. стр. 114).

Об отказоустойчивом кластере Kaspersky Security Center

Отказоустойчивый кластер Kaspersky Security Center 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 Kaspersky Security Center все службы Kaspersky Security Center управляются автоматически. Не пытайтесь перезапускать службы вручную.

Аппаратные и программные требования

Для развертывания отказоустойчивого кластера Kaspersky Security Center 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. Вам нужно предоставить выделенный компьютер, который будет выступать в качестве файлового сервера.

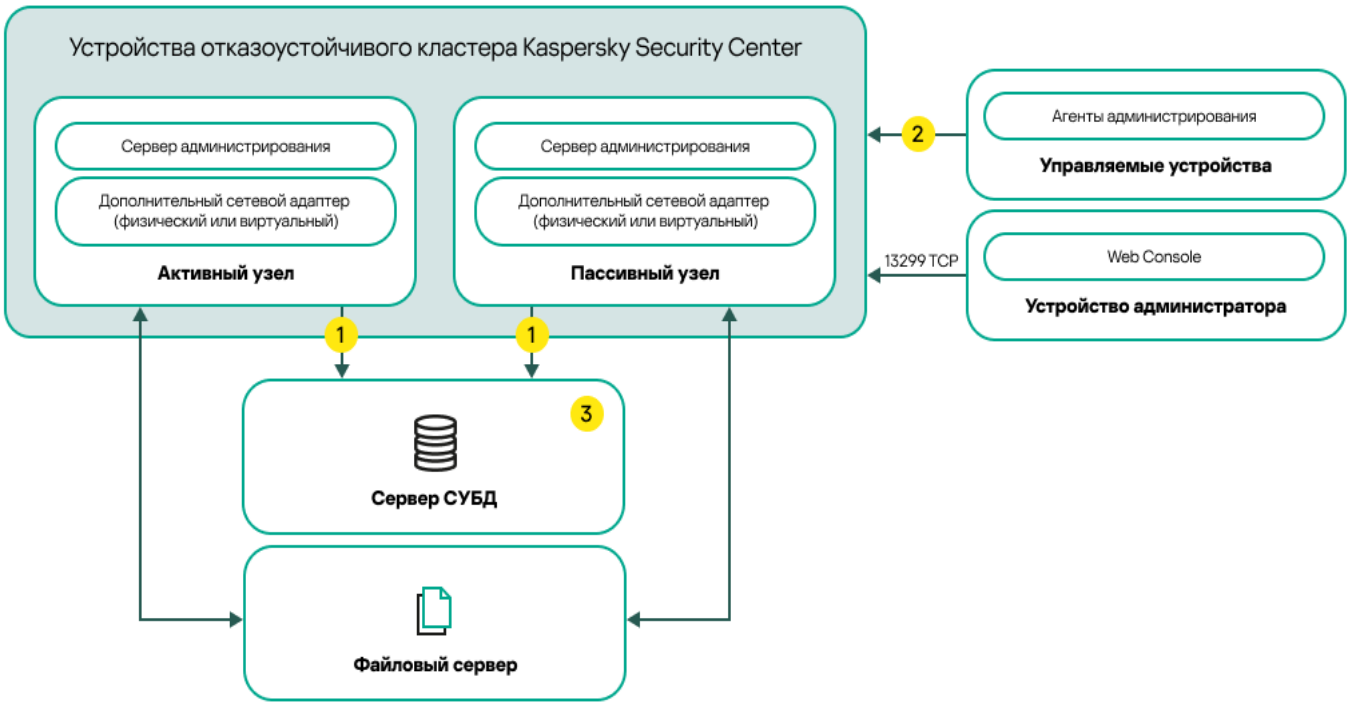
Убедитесь, что вы обеспечили высокую пропускную способность сети между файловым сервером, активным и пассивным узлами.

- Компьютер с системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, выделенный компьютер для этой цели не требуется.

Схемы развертывания

Вы можете выбрать одну из следующих схем развертывания отказоустойчивого кластера Kaspersky Security Center:

- Схема, в которой используется дополнительный сетевой адаптер.
- Схема, в которой используется сторонняя балансировка нагрузки.

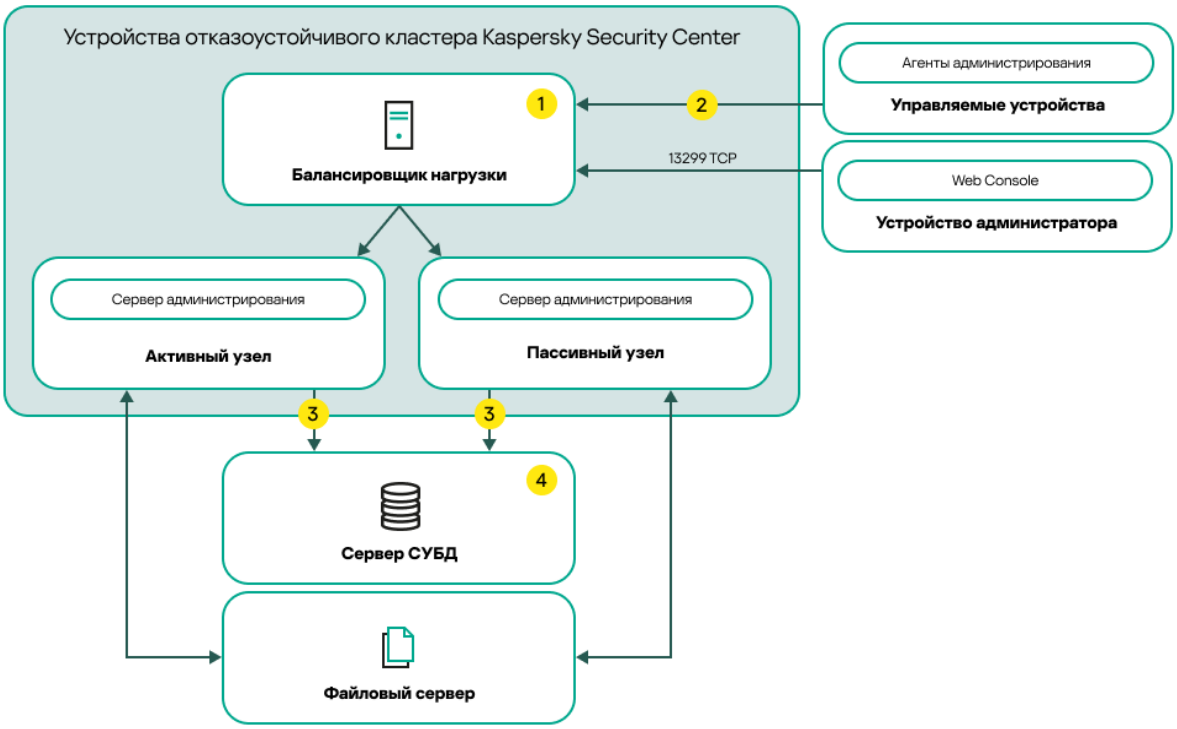


Условные обозначения схемы:

1 Сервер администрирования передает данные в базу данных. Откройте необходимые порты на устройстве, на котором расположена база данных, например порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server. Подробную информацию см. в документации СУБД.

2 На управляемых устройствах откройте следующие порты: TCP 13000, UDP 13000 и TCP 17000.

3 Компьютер с системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, выделенный компьютер для этой цели не требуется. Установите кластер MariaDB Galera на каждый из узлов.



Условные обозначения схемы:

1 На сервере устройства балансировки нагрузки откройте все порты Сервера администрирования: TCP 13000, UDP 13000, TCP 13291, TCP 13299 и TCP 17000.

2 На управляемых устройствах откройте следующие порты: TCP 13000, UDP 13000 и TCP 17000.

3 Сервер администрирования передает данные в базу данных. Откройте необходимые порты на устройстве, на котором расположена база данных, например порт 3306 для MySQL Server или порт 1433 для Microsoft SQL Server. Подробную информацию см. в документации СУБД.

4 Компьютер с системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, выделенный компьютер для этой цели не требуется. Установите кластер MariaDB Galera на каждый из узлов.

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. 123).
- 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 Kaspersky Security Center

Файловый сервер работает как обязательный компонент отказоустойчивого кластера Kaspersky Security Center (см. стр. 114).

► *Чтобы подготовить файловый сервер:*

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям (см. стр. 114).
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. 93).

   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
*\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
sudo sh -c "echo /mnt/KlFocDataShare_klfoc
*\(rw,exec,sync,no_subtree_check,no_root_squash\) >> /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 Kaspersky Security Center, следуйте инструкциям этого сценария (см. стр. 113).

kaspersky

См. также:

Об отказоустойчивом кластере Kaspersky Security Center 114

Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center 113

Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center

Подготовьте два компьютера к работе в качестве активного и пассивного узла для отказоустойчивого кластера Kaspersky Security Center (см. стр. 114).

► *Чтобы подготовить узлы для отказоустойчивого кластера Kaspersky Security Center:*

1. Убедитесь, что у вас есть два компьютера, соответствующих аппаратным и программным требованиям (см. стр. 114). 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
   {сервер}:{путь к папке KlFocStateShare} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw,exec
   {сервер}:{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,nolock,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,exec 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 с помощью стандартных инструментов операционной системы. Если вы хотите использовать виртуальный сетевой адаптер, создайте его с помощью приложений 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 конфигурационный профиль:

     ```
     nmcli connection add type macvlan dev <физический интерфейс> mode
     bridge ifname <виртуальный интерфейс> ipv4.addresses <маска
     адреса> 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 <название 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 Kaspersky Security Center, следуйте инструкциям сценария (см. стр. 113).

См. также:

Об отказоустойчивом кластере Kaspersky Security Center 114
Сценарий: развертывание отказоустойчивого кластера Kaspersky Security Center 113

Установка Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center

Эта процедура описывает, как установить Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center (см. стр. 114). Kaspersky Security Center устанавливается на оба узла отказоустойчивого кластера Kaspersky Security Center по отдельности. Сначала вы устанавливаете приложение 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".

Только пользователь из 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. 22).
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. 368) 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 256 символов.

Пользователь добавлен, и Kaspersky Security Center установлен на 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. 22).
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. 368) 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.

kaspersky

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 Kaspersky Security Center, чтобы убедиться, что вы корректно его настроили и кластер работает правильно.

Запуск и остановка узла кластера вручную

Вам может потребоваться остановить весь отказоустойчивый кластер Kaspersky Security Center 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:

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 приложения установки Сервера администрирования (инсталлятора).
  - **Вручную**. Можно использовать приложение стороннего производителя 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. 125).

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. 127).

Таблица 18. Права роли Postgres

Автоматическое создание базы данных		Создание базы данных вручную
Пользователю *Postgres* не требуются дополнительные права.	Privileges for a new role: CREATEDB.	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.

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. Приложение установки Сервера администрирования (далее также приложение 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 grants for '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. 93).

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

См. также:

Сценарий: управление приложениями 654

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. 93).

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";
   ```

   Если возникает ошибка "New encoding (UTF8) is incompatible with the encoding of the template database", создайте базу данных с помощью команды:
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;
   ```
   вместо:
   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "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. 93).

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

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 14 Web Console, а также как обновить сертификат Сервера администрирования, если Сервер взаимодействует с Kaspersky Security Center 14 Web Console.

kaspersky

В этом разделе

О сертификатах Kaspersky Security Center

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

- 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. 106). 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. 134).

В случае если сертификат Сервера администрирования утерян, для его восстановления необходимо провести переустановку компонента Сервер администрирования и восстановление данных (см. стр. 190).

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 доверенного центра сертификации для автоматически сгенерированных пользовательских сертификатов ("MCA"). Кроме того, в свойствах Сервера администрирования можно указать пользовательские сертификаты, выпущенные другим доверенным центром сертификации, при условии, что интеграция с инфраструктурой открытых ключей (PKI) вашей организации позволяет выпускать сертификаты клиентов с помощью центра сертификации домена.

kaspersky

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 ("С").

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 потому, что сертификат Kaspersky Security Center Web Console является самоподписанным и автоматически генерируется Kaspersky Security Center. Чтобы удалить это предупреждение, можно выполнить одно из следующих действий:

- Замените сертификат Kaspersky Security Center Web Console (см. стр. 133) на пользовательский сертификат (рекомендуемый параметр). Создайте доверенный сертификат, для вашей инфраструктуры и который соответствует требованиям для пользовательских сертификатов (см. стр. 131).
- Добавить сертификат 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 131

Сценарий: задание пользовательского сертификата Сервера администрирования 134

Начало работы 87

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования 82

Веб-сервер 53

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. 129).

Таблица 19. 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: Отсутствует. 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.	—
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:

Сценарий: задание пользовательского сертификата Сервера администрирования 134

Начало работы 87

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

Если вы выбрали создать сертификат, при открытии Kaspersky Security Center Web Console, браузер может информировать вас о том, что подключение к Kaspersky Security Center Web Console не является приватным и что сертификат Kaspersky Security Center 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. 131).
- Добавьте сертификат Kaspersky Security Center 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:*

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. 104).
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления (см. стр. 104).

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 приложения 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. 106), 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. 104).
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления (см. стр. 104).

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. 133).

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.

kaspersky

Предварительные требования

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен доверенным 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: Отсутствует.

    Значение ограничения длины пути может быть целым числом, отличным от "None", но не должно быть меньше 1.
- Использование ключа:
  - 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 доверенным 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. 136).

f. 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. 137).

kaspersky

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 129

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center 131

Начало работы 87

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 20. 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.

Параметр	Значение
`-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 доверенным центром сертификации (англ. certificate authority, CA). Чтобы изменить длину ключа шифрования для сертификатов типа C или CR, укажите `-o RsaKeyLen:<key length>` в утилите klsetsrvcert, где параметр `<key length>` – это требуемая длина ключа. Иначе используется текущая длина ключа сертификата.
`-g <dnsname>`	Сертификат будет создан с указанным DNS-именем.
`-r <calistfile>`	Список доверенных корневых сертификатов, подписанных доверенным 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. 129):

```
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. 137).

Чтобы не потерять соединения Агентов администрирования, используйте следующие команды:

1. Чтобы установить новый сертификат,

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

2. Чтобы указать дату применения нового сертификата,

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

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

См. также:

Сценарий: задание пользовательского сертификата Сервера администрирования.....134

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. 136).

► *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.

Чтобы злоумышленники не могли вывести устройства из-под контроля вашего Сервера администрирования, настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль для удаления** (см. стр. 425).

Утилита klmover требует прав локального администратора. Защиту паролем для запуска утилиты klmover можно не устанавливать для устройств, работающих без прав локального администратора.

При включении параметра **Использовать пароль для удаления** также включается защита паролем в утилите удаления (cleaner.exe).

Описание параметров утилиты klmover представлено в таблице ниже.

Таблица 21. 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.....134

Перевыпуск сертификата Веб-сервера

Сертификат Веб-сервера (см. стр. 271) используемый в Kaspersky Security Center необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства. В зависимости от текущей конфигурации приложения в качестве сертификата Веб-сервера могут использоваться различные сертификаты (подробнее см. О сертификатах Kaspersky Security Center стр. 129).

► *Чтобы перевыпустить сертификат Веб-сервера:*

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 **Сертификаты**.
3. Если вы планируете и дальше использовать сертификат, выданный Kaspersky Security Center:
   a. Выберите вариант **Сертификат, выданный Сервером администрирования** и нажмите на кнопку **Обзор**.
   b. В открывшемся окне блоках параметров **Адрес подключения** и **Срок активации** выберите соответствующие параметры и нажмите на кнопку **ОК**.

Если вы планируете использовать собственный сертификат, выполните следующее:

a. Проверьте, соответствует ли ваш пользовательский сертификат требованиям Kaspersky Security Center (см. стр. 131). При необходимости измените сертификат.
b. Выберите вариант **Другой сертификат**, нажмите на кнопку **Управление сертификатом** и в открывшемся окне нажмите на кнопку **Обзор**.
c. В открывшемся окне в поле **Тип сертификата** выберите тип вашего сертификата:
   - Если вы выбрали **Контейнер PKCS#12**, нажмите на кнопку **Обзор** рядом с полем **Сертификат** и укажите файл сертификата на жестком диске. Если файл сертификата защищен паролем, введите пароль в поле **Пароль (если есть)**.
   - Если вы выбрали **X.509-сертификат**, нажмите на кнопку **Обзор** рядом с полем **Закрытый ключ** и укажите закрытый ключ на жестком диске. Если закрытый ключ защищен паролем, введите пароль в поле **Пароль (если есть)**.
d. Нажмите на кнопку **Сохранить** и далее на кнопку **ОК**.

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 приложение Kaspersky Security Center Web Console и выход из него

Вы можете войти в Kaspersky Security Center Web Console после установки Сервера администрирования и Kaspersky Security Center Web Console (см. стр. 91). Вам нужно 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 приложение.

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:

   - Чтобы войти на Сервер администрирования с доменной учетной записью пользователя, введите имя пользователя и пароль доменного пользователя.

     Вы можете ввести имя доменного пользователя в одном из следующих форматов:

     - `Username@dns.domain`
     - `NTDOMAIN\Username`

     > Прежде чем войти в систему с доменной учетной записью пользователя, опросите контроллеры домена, чтобы получить список пользователей домена (см. стр. 205).

   - Чтобы войти на Сервер администрирования, указав имя пользователя и пароль администратора, введите имя пользователя и пароль внутреннего пользователя.
   - 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. 181).

     c. Введите имя пользователя и пароль администратора, имеющего права на виртуальном Сервере администрирования.

4. 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 окне приложения перейдите в параметры своей учетной записи и выберите **Выйти**.

Приложение Kaspersky Security Center Web Console закрыто, отображается страница входа в приложение.

kaspersky

Интерфейс Kaspersky Security Center Web Console

Управление Kaspersky Security Center осуществляется через интерфейс Kaspersky Security Center Web Console.

Окно приложения Kaspersky Security Center Web Console содержит следующие элементы:

- главное меню в левой части окна;
- рабочая область в правой части окна.

Главное меню

Главное меню содержит следующие разделы:

- **Сервер администрирования**. Отображает имя Сервера администрирования, к которому вы сейчас подключены. Нажмите на значок параметров (), чтобы открыть свойства Сервера администрирования (см. стр. 173).
- **Мониторинг и отчеты**. Предоставляет сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.
- **Активы (Устройства)**. Содержит инструменты для активов, а также задачи (см. стр. 452) и политики приложений "Лаборатории Касперского" (см. стр. 400).
- **Пользователи и роли**. Позволяет управлять пользователями и ролями (см. стр. 475), настраивать права пользователей, назначать пользователям роли и связывать профили политик с ролями.
- **Операции**. Содержит различные параметры, включая лицензирование приложений, просмотр и управление зашифрованными дисками и событиями шифрования, а также управление приложениями сторонних производителей (см. стр. 325). Раздел также предоставляет вам доступ к хранилищам приложений (см. стр. 638).
- **Обнаружение устройств и развертывание**. Позволяет опрашивать сеть (см. стр. 198) для обнаружения клиентских устройств и распределять устройства по группам администрирования вручную или автоматически. Этот раздел содержит мастер первоначальной настройки и мастер развертывания защиты.
- **Marketplace**. Содержит информацию о бизнес-решениях "Лаборатории Касперского", позволяет выбрать нужные вам и перейти к приобретению этих решений на сайте "Лаборатории Касперского".
- **Параметры**. Позволяет создавать резервную копию данных текущего состояния веб-плагина (см .стр. 335), чтобы впоследствии можно было восстановить сохраненное состояние (см. стр. 543). Содержит личные параметры, связанные с внешним видом интерфейса, такие как язык интерфейса (см. стр. 142) или тема.
- **Меню вашей учетной записи**. Содержит ссылку на справку Kaspersky Security Center. Также вы можете выйти из Kaspersky Security Center и просмотреть версию Kaspersky Security Center Web Console и список установленных веб-плагинов управления.

Рабочая область

В рабочей области отображается выбранная вами информация для просмотра в разделах окна интерфейса Kaspersky Security Center Web Console. Она также содержит элементы управления, которые можно использовать для настройки отображения информации.

kaspersky

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 приложения перейдите в раздел **Параметры** → **Язык**.
2. Выберите необходимый язык интерфейса.

Закрепление и отмена закрепления разделов главного меню

Вы можете закрепить разделы Kaspersky Security Center Web Console, чтобы добавить их в избранное и быстро получить к ним доступ из раздела **Закрепленное** в главном меню.

Если закрепленных элементов нет, раздел **Закрепленное** не отображается в главном меню.

Вы можете закрепить разделы, в которых отображаются только страницы. Например, если вы перейдете в раздел **Активы (Устройства)** → **Управляемые устройства**, откроется страница с таблицей устройств, что означает, что вы можете закрепить раздел **Управляемые устройства**. Если после выбора раздела в главном меню отображается окно или элемент не отображается, то закрепить такой раздел невозможно.

► *Чтобы закрепить раздел:*

1. В главном меню наведите курсор мыши на раздел, который вы хотите закрепить.

   Отображается значок булавки ().
2. Нажмите на значок булавки ().

Раздел закреплен и отображается в разделе **Закрепленное**.

Максимальное количество элементов, которые вы можете закрепить, равно пяти.

Вы также можете удалить элементы из избранных, отменив их закрепление.

► *Чтобы отменить закрепление раздела:*

1. В главном окне приложения перейдите в раздел **Закрепленное**.
2. Наведите курсор мыши на раздел, для которого вы хотите отменить закрепление и нажмите на значок отмены закрепления ().

Раздел удален из избранных.

Мастер первоначальной настройки

Приложение 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 приложение 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 приложений (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 приложений, 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.

Приложение 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 вкладке **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

В этом разделе

См. также:

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 приложений "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 (см. стр. 176).

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 приложениями 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 приложений "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 приложений

Выберите плагины для управляемых приложений 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 приложений "Лаборатории Касперского" вручную позднее без запуска мастера первоначальной настройки.

Мастер первоначальной настройки автоматически установит выбранные плагины. Для установки некоторых плагинов вам нужно 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 приложения для языка Kaspersky Security Center отсутствует, выбирается дистрибутив на английском языке.

Чтобы завершить загрузку некоторых дистрибутивов вам нужно принять Лицензионное соглашение. При нажатии кнопки **Принять** отображается текст Лицензионного соглашения. Чтобы перейти к следующему шагу мастера, вам нужно 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 приложений "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 приложения, установленные на клиентских устройствах, в автоматическом режиме будут предоставлять

информацию об их работе Kaspersky Security Network (см. стр. 445). 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 приложения 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. 446).

Шаг 8. Выбор способа активации приложения

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 приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если вы выбрали этот вариант активации приложения, 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 приложение.

  Файл ключа отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

  Чтобы активировать приложение с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если вы выбрали этот вариант активации приложения, 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 приложения

Если вы отложили активацию приложения, 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. Указание параметров управления обновлениями приложений сторонних производителей

Шаг **Параметры управления обновлениями** мастера первоначальной настройки не отображается, если у вас нет лицензии на Системное администрирование (см. стр. 370), а задача *Поиск уязвимостей и требуемых обновлений* уже существует.

Для обновлений приложений сторонних производителей выберите один из следующих вариантов:

- **Search for required updates**

  Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически, если она еще не создана.

  По умолчанию этот вариант выбран.

- **Find and install required updates**

Задачи *Поиск уязвимостей и требуемых обновлений* и *Установка требуемых обновлений и закрытие уязвимостей* создаются автоматически, если они не были созданы ранее.

Этот параметр доступен при наличии лицензии на Системное администрирование (см. стр. 370).

Для обновлений Центра обновления Windows выберите **Использовать источники обновлений, определенные в политике домена.**

Вы можете создать задачи *Поиск уязвимостей и требуемых обновлений* (см. стр. 682) и *Установка требуемых обновлений и закрытие уязвимостей (см. стр. 689)* позднее без запуска мастера первоначальной настройки.

См. также:

Шаг 10. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

Для перехода на следующий шаг мастера дождитесь окончания создания политик и задач.

kaspersky

Шаг 11. Настройка параметров отправки уведомлений по электронной почте

Настройте параметры рассылки оповещений о событиях, регистрируемых при работе приложений "Лаборатории Касперского" на клиентских устройствах. Эти параметры будут использоваться в качестве значений по умолчанию в политиках приложений.

Для настройки рассылки оповещений о возникающих событиях приложений "Лаборатории Касперского" доступны следующие параметры:

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым приложение 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 тестовое сообщение**.

Шаг 12. 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 приложений безопасности или Агента администрирования на устройства в вашей сети (см. стр. 150).

Мастер развертывания защиты

Для установки приложений "Лаборатории Касперского" можно воспользоваться мастером развертывания защиты. Мастер развертывания защиты позволяет проводить удаленную установку приложений как с использованием специально созданных инсталляционных пакетов, так и напрямую из дистрибутивов.

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки приложения (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 приложения 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 приложения**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 358) и настройте Агент администрирования.

В этом разделе

См. также:

Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

► *Чтобы запустить мастер развертывания защиты вручную,*

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

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

kaspersky

Шаг 1. Выбор инсталляционного пакета

Выберите инсталляционный пакет приложения, которое требуется установить.

Если инсталляционный пакет требуемого приложения не содержится в списке, нажмите на кнопку **Добавить** и выберите приложение из списка.

См. также:

Мастер развертывания защиты 150

Сценарий: развертывание приложений "Лаборатории Касперского" 333

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 информацию о лицензионном ключе.

См. также:

Мастер развертывания защиты 150

Сценарий: развертывание приложений "Лаборатории Касперского" 333

kaspersky

Шаг 3. Выбор версии Агента администрирования

Если вы выбрали инсталляционный пакет приложения, отличное от Агента администрирования, необходимо также установить Агент администрирования для подключения приложения к Серверу администрирования Kaspersky Security Center.

Выберите последнюю версию Агента администрирования.

Шаг 4. Выбор устройств

Укажите список устройств, на которые требуется установить приложение:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки приложения 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 150

Сценарий: развертывание приложений "Лаборатории Касперского" 333

Шаг 5. Задание параметров задачи удаленной установки

На странице **Параметры задачи удаленной установки** настройте параметры удаленной установки приложения.

В блоке параметров **Принудительная загрузка инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

- **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 параметр **С помощью Агента администрирования** включен, 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 приложение 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 приложения 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 приложение, если оно уже установлено**

  Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

  Если этот параметр выключен, приложение будет установлено в любом случае.

  По умолчанию параметр включен.

- **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

  Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

  Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

  По умолчанию параметр выключен.

Шаг 6. Управление перезагрузкой

Укажите действие, которое требуется выполнить, если необходимо перезагрузить операционную систему во время установки приложения:

- **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).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**

    Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

    По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

    Если параметр выключен, предложение перезагрузки отображается только один раз.

  - **Принудительно перезагрузить через (мин)**

    После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

    По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

  - **Принудительно закрывать приложения в заблокированных сеансах**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения 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 приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Шаг 7. Удаление несовместимых приложений перед установкой

Этот шаг присутствует, только если приложение, которое вы разворачиваете, несовместимо с другими приложениями.

Выберите этот параметр, если вы хотите, чтобы приложение Kaspersky Security Center автоматически удаляло несовместимые приложения с приложением, которое вы устанавливаете.

Отображается список несовместимых приложений.

Если этот параметр не выбран, приложение будет установлено только на устройствах, на которых нет несовместимых приложений.

Шаг 8. Перемещение устройств в папку Управляемые устройства

Укажите, следует ли перемещать устройства в группу администрирования после установки Агента администрирования.

- **Не перемещать устройства**

  Устройства остаются в тех группах, к которым они принадлежат. Устройства, не принадлежащие ни к одной из групп, остаются нераспределенными.

- **Переместить нераспределенные устройства в группу**

  Устройства перемещаются в выбранную вами группу администрирования.

По умолчанию выбран вариант **Не перемещать устройства**. По соображениям безопасности вы можете предпочесть перемещение устройств вручную.

Шаг 9. Выбор учетных записей для доступа к устройствам

Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной установки:

- **Учетная запись не требуется (Агент администрирования уже установлен)**

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. 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 приложения.

Чтобы указать учетную запись пользователя, под которой будет запускаться приложение 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 10. Запуск установки

Это последний шаг мастера. На этом шаге задача **Удаленная установка** была успешно создана и настроена.

По умолчанию параметр **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, задача **Удаленная установка** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, задача **Удаленная установка** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

Нажмите на кнопку **ОК**, чтобы завершить последний шаг мастера развертывания защиты.

kaspersky

Обновление предыдущей версии Kaspersky Security Center

Вы можете установить Сервер администрирования версии 15.1 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 13). При обновлении до версии 15.1 все данные и параметры предыдущей версии Сервера администрирования сохраняются.

Перед обновлением Kaspersky Security Center убедитесь, что вы используете те версии операционной системы и СУБД, которые поддерживаются Сервером администрирования версии 15.1 (см. стр. 22). При необходимости вы можете перенести Сервер администрирования на другое устройство с более поздними версиями операционной системы и СУБД (см. стр. 188).

Вы можете обновить версию Сервера администрирования одним из следующих способов:

- С помощью установочного файла Kaspersky Security Center (см. стр. 159).
- Создав резервную копию данных Сервера администрирования, установив новую версию Сервера администрирования и восстановив данных Сервера администрирования из резервной копии (см. стр. 160).

Во время обновления недопустимо совместное использование СУБД Сервером администрирования и каким-либо другим приложением.

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

Также вам необходимо обновить Kaspersky Security Center Web Console до новой версии (см. стр. 163).

Обратите внимание, если вы обновите Сервер администрирования до версии 15.1, вы не сможете создавать инсталляционные пакеты Агента администрирования версии 15 или ниже. Ранее созданные инсталляционные пакеты будут доступны.

При обновлении предыдущей версии Kaspersky Security Center все установленные плагины поддерживаемых приложений "Лаборатории Касперского" сохраняются. Плагины Сервера администрирования и Агента администрирования обновляются автоматически. Перед началом обновления рекомендуется создать резервную копию данных Сервера администрирования (см. стр. 190).

kaspersky

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 15.1 вы можете установить новую версию поверх предыдущей с помощью установочного файла Kaspersky Security Center.

► *Чтобы обновить Сервер администрирования предыдущей версии до версии 15.1 с помощью установочного файла:*

1. Загрузите установочный файл Kaspersky Security Center с полным пакетом для версии 15.1 с сайта "Лаборатории Касперского":
   - Для устройств с операционной системой на базе RPM: ksc64-<номер версии>.x86_64.rpm.
   - Для устройств с операционной системой на основе Debian: ksc64_<номер версии>_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>.x86_64.rpm
   ```

   - Для устройств с операционной системой на основе Debian:

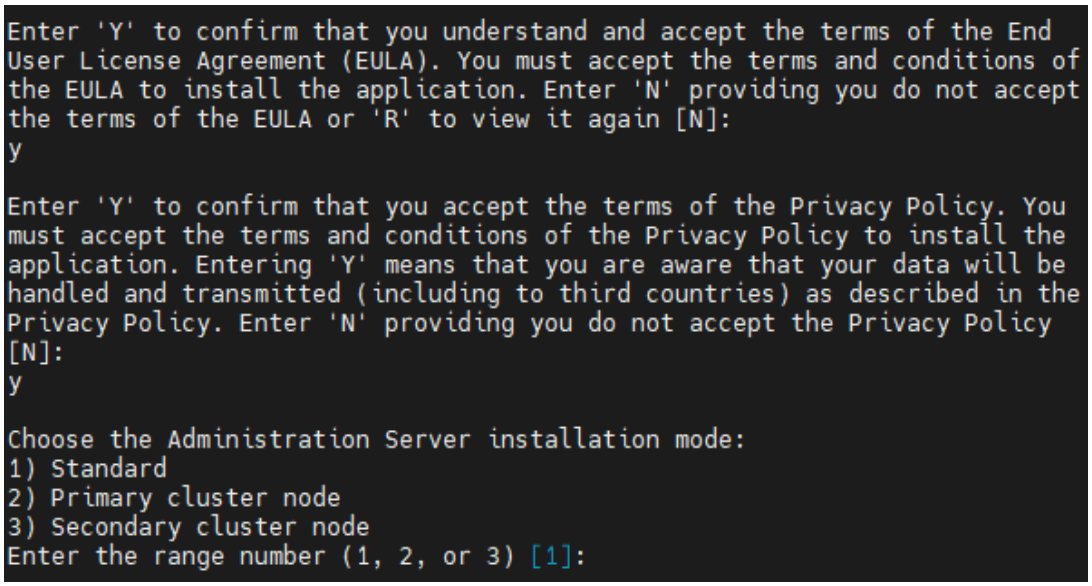
   ```
   $ sudo dpkg -i ksc64_<номер версии>_amd64.deb
   ```

   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 приложения 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 160

Обновление предыдущей версии Kaspersky Security Center с помощью резервной копии

Для обновления Сервера администрирования с предыдущей версии (начиная с версии 13) до версии 15.1 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 15.1 с помощью резервной копии данных:*

1. Перед обновлением, выполните резервное копирование данных Сервера администрирования старой версии приложения (см. стр. 190).
2. Удалите старую версию Kaspersky Security Center.
3. Установите Kaspersky Security Center версии 15.1 на бывшем Сервере администрирования (см. стр. 87).
4. Восстановите данные Сервера администрирования из резервной копии данных, созданной перед обновлением (см. стр. 190).
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.....159

Обновление Kaspersky Security Center на узле отказоустойчивого кластера Kaspersky Security Center

Вы можете установить Сервер администрирования версии 15.1 на каждый узел отказоустойчивого кластера Kaspersky Security Center, где установлен Сервер администрирования более ранней версии (начиная с версии 14). При обновлении до версии 15.1 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. 159) или с помощью резервной копии (см. стр. 160).

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

1. Загрузите установочный файл Kaspersky Security Center с полным пакетом для версии 15.1 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. 123).
3. Отключите общие папки для кластера и подключите их с помощью параметров, указанных в разделе Подготовка файлового сервера для отказоустойчивого кластера Kaspersky Security Center (см. стр. 117).
4. Повторно сопоставьте точки подключения и общие папки на узлах кластера, как описано в разделе Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center (см. стр. 118).
5. 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
     ```

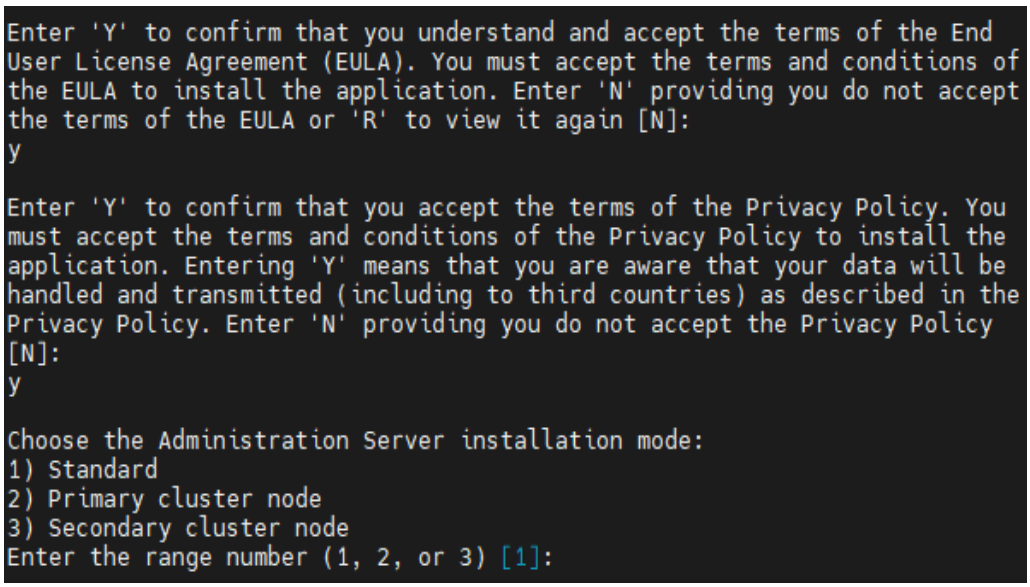
   После успешного выполнения команды создается скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Сообщение об этом отображается в терминале.
6. Запустите скрипт /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl для настройки обновленного Сервера администрирования.
7. Прочтите Лицензионное соглашение 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 приложения будет продолжена после того, как вы дважды введете "Y".
8. 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.

9. Выполните шаги 3–5 на пассивном узле.

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

10. Запустить кластер (см. стр. 123).

    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 Kaspersky Security Center.

Обновление Kaspersky Security Center Web Console

В этом разделе описано, как обновить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) на устройствах с операционными системами Linux.

Если вам нужно обновить Kaspersky Security Center Web Console на Astra Linux в режиме замкнутой программной среды, следуйте инструкциям для Astra Linux (см. стр. 165).

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 обновить Kaspersky Security Center Web Console:*

1. Убедитесь, что на устройстве, на котором вы хотите обновить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.
2. Прочитайте и примите 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 принимаете условия Лицензионного соглашения, не обновляйте Kaspersky Security Center Web Console с помощью установочного файла.
3. Используйте тот же файл ответов, который вы подготовили перед установкой Kaspersky Security Center Web Console (см. стр. 106). Имя файла ответов ksc-web-console-setup.json. Файл расположен в директории /etc/ksc-web-console-setup.json.

   Если файл ответов не существует, создайте новый файл ответов, содержащий параметры подключения Kaspersky Security Center Web Console к Серверу администрирования (см. стр. 106). Назовите файл ksc-web-console-setup.json и расположите его в директории /etc.

   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
   }
   ```

   Если вы хотите обновить приложение Kaspersky Security Center Web Console , подключенное к Серверу администрирования, который установлен на узлах отказоустойчивого кластера Kaspersky Security Center, в файле ответа (см. стр. 106) укажите `доверенный` параметр установки, чтобы разрешить отказоустойчивому кластеру Kaspersky Security Center 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 Kaspersky Security Center (см. стр. 118). 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 Kaspersky Security Center (см. стр. 117). 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 Kaspersky Security Center, которое будет отображаться в окне входа в Kaspersky Security Center Web Console.

> Приложение Kaspersky Security Center Web Console невозможно обновить с помощью того же установочного файла .rpm. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки приложения, вам нужно сначала удалить приложение, а затем установить его 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 обновить предыдущую версию Kaspersky Security Center Web Console, выполните одну из следующих команд:

   - Для устройств с операционной системой на основе RPM:

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

   - Для устройств с операционной системой на основе Debian:

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

   Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки.

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

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

После завершения обновления вы можете использовать браузер, чтобы открыть Kaspersky Security Center Web Console и осуществить вход (см. стр. 139).

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

В этом разделе описано, как обновить Сервер Kaspersky Security Center Web Console (далее также Kaspersky Security Center Web Console) на устройствах с операционной системой Astra Linux Special Edition.

► *Чтобы обновить Kaspersky Security Center Web Console:*

1. Убедитесь, что на устройстве, на котором вы хотите обновить Kaspersky Security Center Web Console, работает один из поддерживаемых дистрибутивов Linux.
2. Прочитайте и примите 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 принимаете условия Лицензионного соглашения, не обновляйте Kaspersky Security Center Web Console с помощью установочного файла.
3. Используйте тот же файл ответов, который вы подготовили перед установкой Kaspersky Security Center Web Console (см. стр. 106). Имя файла ответов ksc-web-console-setup.json. Файл расположен в директории /etc/ksc-web-console-setup.json.

   Если файл ответов не существует, создайте новый файл ответов, содержащий параметры подключения Kaspersky Security Center Web Console к Серверу администрирования (см. стр. 106). Назовите файл ksc-web-console-setup.json и расположите его в директории /etc.

   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. Убедитесь, что в файле `/etc/digsig/digsig_initramfs.conf` параметр `DIGSIG_ELF_MODE` указан следующим образом:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Убедитесь, что установлен пакет совместимости `astra-digsig-oldkeys`.

   Если этот пакет не установлен, выполните следующую команду:

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

6. Создайте директорию для ключа приложения, если ее не существует:

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

7. Поместите ключ приложения 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 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.

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

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

После завершения обновления вы можете использовать браузер, чтобы открыть Kaspersky Security Center Web Console и осуществить вход (см. стр. 139).

kaspersky

Перенос данных в приложение Kaspersky Security Center

Следуя этому сценарию, вы можете переместить структуру групп администрирования, включая управляемые устройства и другие объекты группы (политики, задачи, глобальные задачи, теги и выборки устройств) из Kaspersky Security Center Windows под управление Kaspersky Security Center.

Ограничения:

- Перенос данных возможен только из Kaspersky Security Center 14.2 Windows в Kaspersky Security Center начиная с версии 15.
- Вы можете выполнить этот сценарий только с помощью Kaspersky Security Center Web Console.

Прежде чем начать, узнайте больше о функциях и ограничениях Kaspersky Security Center:

- Функциональные различия Kaspersky Security Center Windows и Kaspersky Security Center (см. стр. 34)
- Список приложений "Лаборатории Касперского" поддерживаемых приложением Kaspersky Security Center (см. стр. 33)

Этапы

Сценарий переноса данных состоит из следующих этапов:

1. Выберите способ переноса данных

   Вы переносите данные в Kaspersky Security Center с помощью мастера переноса данных. Действия мастера переноса данных зависят от того, организованы ли Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center в иерархию:

   - 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 управляете процессом переноса данных и переключаетесь между Серверами в рамках одного экземпляра Kaspersky Security Center Web Console. Если вы предпочитаете этот вариант, вы можете организовать Серверы администрирования в иерархию, чтобы упростить процедуру переноса данных. Для этого создайте иерархию перед началом переноса данных.

   - Перенос данных с помощью файла экспорта (ZIP-архив)

     Выберите этот параметр, если Серверы администрирования Kaspersky Security Center Windows и Kaspersky Security Center не выстроены в иерархию. Вы управляете процессом переноса данных с помощью двух экземпляров Kaspersky Security Center Web Console, одного экземпляра Kaspersky Security Center Windows и другого Kaspersky Security Center. В этом случае вы будете использовать файл экспорта, который вы создали и загрузили во время экспорта из Kaspersky Security Center Windows (см. стр. 169), и импортировать этот файл в Kaspersky Security Center (см. стр. 170).

g. **Экспорт данных из Kaspersky Security Center Windows**

   Откройте Kaspersky Security Center Windows и запустите мастер переноса данных (см. стр. 169).

h. **Импорт данных в приложение Kaspersky Security Center**

   Продолжите работу мастера переноса данных, чтобы импортировать экспортированные данные в Kaspersky Security Center (см. стр. 170). Если Серверы организованы в иерархию, импорт начинается автоматически после успешного экспорта в том же мастере. Если Серверы не

выстроены в иерархию, вы продолжите работу мастера переноса данных после перехода на Kaspersky Security Center.

i. **Выполнение дополнительных действий для переноса объектов и параметров из Kaspersky Security Center Windows в Kaspersky Security Center вручную (необязательный шаг)**

Вы также можете перенести объекты и параметры, которые невозможно передать с помощью мастера переноса данных. Например, вы можете дополнительно сделать следующее:

- Перенести лицензионные ключи, используемые Сервером администрирования и управляемыми приложениями (см. стр. 377).
- Настроить глобальные задачи Сервера администрирования.
- Настроить параметры политики Агента администрирования (см. стр. 425).
- Создать инсталляционные пакеты приложений (см. стр. 336).
- Создать виртуальные Серверы администрирования (см. стр. 181).
- Назначить и настроить точки распространения (см. стр. 290).
- Создать правила перемещения устройств (см. стр. 276).
- Настроить правила автоматического назначения тегов устройствам (см. стр. 323).
- Создание категории приложений (см. стр. 654)

j. **Переместить импортированные управляемые устройства под управление Kaspersky Security Center**

Завершите перенос данных, переместите импортированные управляемые устройства под управление Kaspersky Security Center. В текущей версии Kaspersky Security Center это можно сделать одним из следующих способов:

- С помощью утилиты klmover (см. стр. 137).

  Используйте утилиту klmover и укажите параметры подключения для нового Сервера администрирования.

- С помощью установки или переустановки Агента администрирования на управляемые устройства.

  Создайте инсталляционный пакет Агента администрирования и укажите параметры подключения для нового Сервера администрирования в свойствах инсталляционного пакета. С помощью инсталляционного пакета установите Агент администрирования на импортированные управляемые устройства с помощью задачи удаленной установки (см. стр. 349). Подробнее см. в разделе Переключение управляемых устройств под управление Kaspersky Security Center (см. стр. 171).

  Вы также можете создать и использовать автономный инсталляционный пакет для локальной установки Агента администрирования (см. стр. 339).

k. **Обновите Агент администрирования до последней версии.**

Рекомендуется обновить Агент администрирования для Linux до той же версии, что и Kaspersky Security Center (см. стр. 518).

l. **Убедитесь, что управляемые устройства видны на новом Сервере администрирования.**

На Сервере администрирования Kaspersky Security Center откройте список управляемых устройств (**Активы (Устройства)** → **Управляемые устройства**) и проверьте значения в столбцах **Видимо**, **Агент администрирования установлен** и **Последнее подключение к Серверу администрирования**.

kaspersky

Другие способы переноса данных

Кроме мастера переноса данных, есть другие способы переноса текущих объектов, но эти способы позволяют переносить только политики и задачи.

- Экспортируйте задачи (см. стр. 462) из Kaspersky Security Center Windows, а затем импортируйте задачи в Kaspersky Security Center (см. стр. 463).
- Экспортируйте определенные политики (см. стр. 414) из Kaspersky Security Center Windows, а затем импортируйте политики в Kaspersky Security Center (см. стр. 414). Связанные профили политик экспортируются и импортируются вместе с выбранными политиками.

См. также:

Экспорт групповых объектов из Kaspersky Security Center Windows 169

Экспорт групповых объектов из Kaspersky Security Center Windows

Для переноса структуры группы администрирования, которая включает управляемые устройства и другие объекты группы из Kaspersky Security Center Windows в Kaspersky Security Center, вам сначала необходимо 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 приложений.
- Глобальные задачи (см. стр. 452)
- Пользовательские выборки устройств.
- Структуру групп администрирования и входящие в нее устройства.
- Теги, назначенные устройствам, данные которых вы переносите (см. стр. 318).

Перед началом экспорта прочтите общую информация о переносе данных в Kaspersky Security Center. 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 приложения перейдите в раздел **Операции** → **Перенос данных**.

3. Выберите **Перенести данные в Kaspersky Security Center или в Kaspersky SMP**, 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 приложения, задачи и политики которых будут экспортированы. Выберите только те приложения, которые поддерживаются Kaspersky Security Center. Объекты неподдерживаемых приложений 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 приложений.

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. 171). Для переноса данных без поддержки иерархии Сервера администрирования вы можете вручную импортировать сохраненный файл экспорта в Kaspersky Security Center (см. стр. 171).

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 (см. стр. 169), вам нужно импортировать ее в приложение Kaspersky Security Center или Kaspersky SMP.

► *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. 169).
   - Если Серверы не выстроены в иерархию:
     a. Откройте Kaspersky Security Center Web Console, подключенный к Kaspersky Security Center или к Kaspersky XDR Expert.
     b. В главном окне приложения 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. 169). 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 невозможно. 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 в перенесенной задаче указаны данные учетной записи, под которой она запускается (см. стр. 456), вам нужно открыть задачу и ввести пароль еще раз после завершения импорта.

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. 171).

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. 137), либо установив Агент администрирования на управляемые устройства с помощью задачи удаленной установки (см. стр. 349).

► *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. 267).

   Если инсталляционный пакет Агента администрирования отсутствует в списке пакетов, загрузите новый (см. стр. 336).

3. На вкладке **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. 349).

   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. 290). 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 приложения.

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 вкладке **Общие** выберите раздел **Порты подключения**.

Будут отображены основные параметры подключения к выбранному Серверу Администрирования.

См. также:

Порты, используемые Kaspersky Security Center.....42

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 приложение, которое взаимодействует с Сервером администрирования через Kaspersky Security Center OpenAPI (см. стр 730). 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. 583) 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 приложений:

- 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, сетевой экран поможет предотвратить вмешательство злоумышленников (см. стр. 42).

- Приложения, взаимодействующие с Сервером администрирования через объекты автоматизации klakaut.

- Приложения, 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 приложения.

Вы можете установить IPv4-адреса и IPv6-адреса. Указать диапазоны IP-адресов невозможно.

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 под учетной записью root:

```
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 ли 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 командную строку под учетной записью root:

```
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

Настройка параметров доступа Сервера администрирования к интернету

Доступ к интернету необходимо настроить, чтобы использовать Kaspersky Security Network и загружать обновления антивирусных баз для Kaspersky Security Center и управляемых приложений "Лаборатории Касперского".

► *Чтобы указать параметры доступа Сервера администрирования к интернету:*

1. В главном меню нажмите на значок параметров () рядом с именем Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Лицензионные ключи**.
3. 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.

Также можно настроить доступ в интернет с помощью мастера первоначальной настройки (см. стр. 144).

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 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.

Главный Сервер администрирования получает данные только от невиртуальных подчиненных Серверов администрирования в рамках перечисленных выше параметров. Это ограничение не распространяется на виртуальные Серверы администрирования, которые совместно используют базу данных со своим главным Сервером 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 вкладку **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. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. 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.

     Этот параметр необходим, если включен параметр **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.
   - **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 прокси-сервера**
     - **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. 738).

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. 131).
- 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 вкладке **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:

Иерархия Серверов администрирования с подчиненным Сервером в демилитаризованной зоне ...83

Иерархия Серверов администрирования: главный Сервер администрирования и подчиненный Сервер администрирования 82

Порты, используемые Kaspersky Security Center.....42

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. 177). После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center Web Console.

Управление виртуальными Серверами администрирования

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

- создание виртуальных Серверов администрирования (см. стр. 181);
- включение и выключение виртуальных Серверов администрирования (см. стр. 182);
- назначение администратора виртуального Сервера администрирования (см. стр. 183);
- смена Сервера администрирования для клиентских устройств (см. стр. 185);
- удаление виртуальных Серверов администрирования (см. стр. 187).

В этом разделе

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования (см. стр. 235).

► *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 вкладку **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**
   - **Адрес подключения Сервера 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 вкладке **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. 177). 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 вкладку **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 187

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. 139). 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. 181).
- 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. 478) 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 именем 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 **ОК**.

   Приложение 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**.

Приложение 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. 511). 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. 494).

Приложение назначает роль учетной записи администратора.

Настройка прав доступа на уровне объекта

В дополнение к назначению прав доступа на уровне функциональной области (см. стр. 478), вы можете настроить доступ к определенным объектам (см. стр. 488) 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 187

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 приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения 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 было установлено и запущено приложение, выполняющее 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. 456).
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 181

Сценарий: настройка защиты сети 393

kaspersky

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 вкладку **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 182

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 вкладке **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 /var/opt/kaspersky/klnagent_srv/logs/sc.syslog.

kaspersky

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение 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 операционной системы. 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 вкладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.
3. Нажмите на кнопку **Сохранить**.

См. также:

О блокировке частых событий.....596

Сценарий: настройка защиты сети.....393

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. 191) с помощью Kaspersky Security Center Web Console или запустите утилиту klbackup (см. стр. 191).

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. 22). Проверьте, что порты, используемые на Сервере администрирования доступны (см. стр. 42).
3. На новом устройстве установите СУБД, которую будет использовать Сервер администрирования.

   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. 93). 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. 93).
5. После завершения установки восстановите данные Сервера администрирования на новом устройстве с помощью утилиты klbackup.
6. Откройте Kaspersky Security Center Web Console и подключитесь к Серверу администрирования (см. стр. 139).
7. Убедитесь, что все клиентские устройства подключены к Серверу администрирования.
8. Удалите Сервер администрирования и сервер баз данных с предыдущего устройства.

См. также:

Смена Сервера администрирования для клиентских устройств 329

Резервное копирование и восстановление данных Сервера администрирования 190

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. Вам нужно 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. 191).
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования (см. стр. 191). Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке приложения (обычно, /opt/kaspersky/ksc64/sbin/klbackup).

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры приложений, сохраненные на Сервере администрирования события);
- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

В этом разделе

См. также:

Обновление предыдущей версии Kaspersky Security Center с помощью резервной копии 160

kaspersky

Создание задачи резервного копирования данных Сервера администрирования

Задача резервного копирования является задачей Сервера администрирования и создается мастером первоначальной настройки (см. стр. 143). 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 приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В списке **Приложение** выберите **Kaspersky Security Center 15** и в списке **Тип задачи** выберите **Резервное копирование данных Сервера администрирования**.
4. На соответствующем шаге 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 шаге **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.

Если вы выполнили резервное копирование данных Сервера администрирования, входящего в состав Kaspersky Security Center 15 или более ранней версии, при использовании СУБД MariaDB более ранней версии, а затем восстановили данные на устройстве с более поздней версией MariaDB, может возникнуть ошибка. Подробную информацию см. в статье Как восстановить данные Сервера администрирования из резервной копии, созданной на более ранней версии СУБД.

► *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] [-cert_only]
```

> 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.

- `-cert_only` – сохранить или восстановить только сертификат и закрытый ключ Сервера администрирования.

Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет освободить место в папке Сервера администрирования и уменьшить объем базы данных за счет удаления ненужных объектов. Это поможет вам повысить производительность и надежность работы приложения. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

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

- Удаляет ненужные папки и файлы из папки хранилища.
- Удаляет ненужные записи из таблиц (также известные как "висячие указатели").
- Очищает кеш.
- Обслуживает базу данных (если вы используете SQL Server или PostgreSQL в качестве СУБД):
  - проверяет базу данных на наличие ошибок (доступно только для SQL Server);
  - перестраивает индексы базы данных;
  - обновляет статистику базы данных;
  - сжимает базу данных (если необходимо).

Задача Обслуживание Сервера администрирования поддерживает MariaDB версии 10.3 и выше. Если используется MariaDB версии 10.2 или ниже, администраторам следует обслуживать базу данных самостоятельно.

Задача Обслуживание Сервера администрирования создается автоматически при установке Kaspersky Security Center. Если задача Обслуживание Сервера администрирования удалена, вы можете создать ее вручную.

► *Чтобы создать задачу Обслуживание Сервера администрирования:*

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

   Запустится мастер создания задачи.
3. В окне мастера **создания задачи** выберите тип задачи **Обслуживание Сервера администрирования** и нажмите на кнопку **Далее**.
4. Следуйте дальнейшим шагам мастера.

В результате созданная задача отобразится в списке задач. Для одного Сервера администрирования может выполняться только одна задача Обслуживание Сервера администрирования. Если задача Обслуживание

Сервера администрирования для Сервера администрирования уже создана, создание еще одной задачи Обслуживание Сервера администрирования невозможно.

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 вкладку **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 и бывшие подчиненные Серверы администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

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 приложение устанавливает TCP/UDP-соединение с DNS-сервером. Если Kaspersky Security Center использует общедоступный DNS-сервер, обработка данных регулируется политикой конфиденциальности соответствующего сервиса.

► *Чтобы настроить использование публичного DNS с помощью утилиты klscflag:*

1. Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
2. Чтобы выключить использование публичного DNS, выполните следующую команду под учетной записью root:

```
klscflag -fset -pv ".core/.independent" -s Transport -n
ForceUseSystemDNS -t d -v 1
```

3. Чтобы включить использование публичного DNS, выполните следующую команду под учетной записью root:

```
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 шифрования 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 доверенным центром сертификации.

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

1. Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, 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 под учетной записью root:

```
klscflag -fset -pv ".core/.independent" -s Transport -n
SrvUseStrictSslSettings -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 предыдущими версиями Kaspersky Security Center). Это значение по умолчанию.

  Наборы шифрования поддерживаемые TLS-протоколом 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 поддерживаемые TLS-протоколом 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 поддерживаемые TLS-протоколом 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 поддерживаемые TLS-протоколом 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:
   - службу Сервера администрирования;

- службу Веб-сервера;
- 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.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

2. Выполните одну из следующих команд в командной строке под учетной записью root:

   - 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 сетевых устройств

Вам нужно выполнить поиск устройств перед установкой приложений 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.

m. Настройка будущих опросов

Убедитесь, что опрос IP-диапазонов (см. стр. 202) 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. 205), если в вашей сети есть IPv6-устройства.

Если сетевые устройства включены в домен, рекомендуется использовать опрос контроллеров домена (см. стр. 205).

n. **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. 276) 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**.

Oiпрос сети Windows

Об опросе сети Windows

При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети. Во время полного опроса с каждого клиентского устройства запрашивается следующая информация:

- Имя операционной системы
- IP-адрес
- DNS-имя
- NetBIOS-имя

Как во время быстрого опроса, так и во время полного опроса необходимо:

- наличие открытых портов UDP 137/138, TCP 139, UDP 445, TCP 445;
- SMB-протокол включен;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на Сервере администрирования;
- служба Microsoft Computer Browser должна использоваться, и устройство, которое выполняет роль основного браузера, должно быть доступно на клиентском устройстве:
  - наличие хотя бы одного устройства, если количество сетевых устройств не превышает 32;
  - наличие как минимум одного устройства на каждые 32 сетевых устройства.

Полный опрос сети может быть запущен, только если быстрый опрос был запущен как минимум один раз.

Просмотр и изменение параметров опроса сети Windows

► *Чтобы изменить параметры опроса сети Windows:*

1. В дереве консоли в папке **Обнаружение устройств** выберите вложенную папку **Домены**.

   Вы можете перейти в папку **Обнаружение устройств** из папки **Нераспределенные устройства** по кнопке **Опросить сейчас**.

   В рабочей области подпапки **Домены** отображается список устройств.

2. Нажмите на кнопку **Опросить сейчас**.

   Откроется окно свойств домена. При необходимости настройте параметры опроса сети Windows:

   - **Включить опрос сети Windows**

     По умолчанию этот вариант выбран. Если не требуется выполнять опрос сети Windows (например, если достаточно опроса Active Directory), можно отменить выбор данного параметра.

   - **Настроить расписание быстрого опроса**

     По умолчанию интервал времени составляет 15 минут.

     При быстром опросе Сервер администрирования получает только информацию о списке NetBIOS-имен устройств всех доменов и рабочих групп сети.

     Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

     Доступны следующие варианты расписания опроса сети:

     - **Каждый N день**

     Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

     - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

     По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

     - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.

     По умолчанию опрос запускается каждую пятницу в 18:00:00.

     - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

     По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

- **Настроить расписание полного опроса**

По умолчанию период опроса составляет один час. Данные, полученные при каждом последующем опросе, полностью замещают предыдущие данные.

Доступны следующие варианты расписания опроса сети:

- **Каждый N день**

Опрос выполняется регулярно, с заданным интервалом в днях, начиная с указанной даты и времени.

По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.

- **Каждые N минут**

Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

По умолчанию опрос запускается каждые пять минут, начиная с текущего системного времени.

- **По дням недели**

Опрос выполняется регулярно, в указанные дни недели, в указанное время.

По умолчанию опрос запускается каждую пятницу в 18:00:00.

- **Ежемесячно, в указанные дни выбранных недель**

Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

По умолчанию дни месяца не выбраны; время начала по умолчанию – 18:00:00.

- **Запускать пропущенные задачи**

Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

По умолчанию параметр включен.

Если требуется запустить опрос сети немедленно, нажмите на кнопку **Опросить сейчас**. Будут запущены оба типа опроса.

На виртуальном Сервере администрирования просмотр и изменение параметров опроса сети Windows осуществляется в окне свойств точки распространения, в разделе **Обнаружение устройств**.

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. 205) устройств.

Просмотр и изменение параметров опроса IP-диапазонов

► *Чтобы просмотреть и изменить параметры опроса IP-диапазонов:*

1. В главном окне приложения 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. 203). 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.

- **Каждые N минут**

  Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.

- **По дням недели**

  Опрос выполняется регулярно, в указанные дни недели, в указанное время.

- **Ежемесячно, в указанные дни выбранных недель**

  Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.

- **Запускать пропущенные задачи**

  Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

  Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

  Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

  По умолчанию параметр выключен.

5. Нажмите на кнопку **Сохранить**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Запуск опроса вручную

► *Чтобы запустить проверку немедленно,*

Нажмите на кнопку **Начать опрос**.

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. 205), Kaspersky Security Center будет опрашивать всю сеть.

► *Чтобы добавить новый IP-диапазон:*

1. В главном окне приложения 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. 202). 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 приложения 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 приложения 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. 208).

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.

Сервер отправляет эхо-запросы ICMP (аналогично команде ping) во время опроса Microsoft Active Directory.

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 приложения 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.
   - **Каждые N минут**

     Опрос выполняется регулярно, с заданным интервалом в минутах, начиная с указанного времени.
   - **По дням недели**

     Опрос выполняется регулярно, в указанные дни недели, в указанное время.
   - **Ежемесячно, в указанные дни выбранных недель**

     Опрос выполняется регулярно, в указанные дни каждого месяца, в указанное время.
   - **Запускать пропущенные задачи**

     Если Сервер администрирования выключен или недоступен в течение времени, на которое запланирован опрос, Сервер администрирования может либо начать опрос сразу после его включения, либо дождаться следующего планового опроса.

     Если этот параметр включен, Сервер администрирования начинает опрос сразу после его включения.

     Если этот параметр выключен, Сервер администрирования ждет следующего планового опроса.

     По умолчанию параметр выключен.

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. 290).
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. 276). 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. 139).

Аутентификация и подключение к контроллеру домена

При первоначальном подключении к контроллеру домена Сервер администрирования идентифицирует протокол подключения. Этот протокол используется для всех будущих подключений к контроллеру домена.

Первоначальное подключение к контроллеру домена происходит следующим образом:

1. Сервер администрирования пытается подключиться к контроллеру домена по TLS.

   По умолчанию проверка сертификата не требуется. Для флага KLNAG_LDAP_TLS_REQCERT установите значение 1, чтобы принудительно выполнить проверку сертификата.

   По умолчанию для доступа к цепочке сертификатов используется зависящий от операционной системы путь к центру сертификации (CA). Используйте флаг KLNAG_LDAP_SSL_CACERT, чтобы указать другой путь.

2. В случае сбоя TLS-соединения Сервер администрирования пытается подключиться к контроллеру домена по SASL (DIGEST-MD5).
3. В случае сбоя подключения по SASL (DIGEST-MD5) Сервер администрирования использует простую проверку подлинности (Simple Authentication) по незашифрованному TCP-соединению для подключения к контроллеру домена.

Вы можете использовать утилиту klscflag для настройки флагов.

Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
Например, следующая команда принудительно проверяет сертификат:

```
klscflag -fset -pv klserver -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

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 контроллером 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.

Если вы хотите правильно опросить контроллер домена Samba, вам нужно указать `netbios name` и параметры `workgroup` в файле `/etc/samba/smb.conf`.

См. также:

Опрос контроллеров домена 205

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. Также несуществующие виртуальные машины могут отображаться в Kaspersky Security Center Web Console.

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. 210).

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 приложения 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 распределенным приложением. В состав Kaspersky Security Center входят следующие приложения:

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Kaspersky Security Center Web Console – основной инструмент администратора. Вы можете установить Kaspersky Security Center Web Console на том же устройстве, что и Сервер администрирования.
- Агент администрирования – служит для управления установленным на устройстве приложением 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 Kaspersky Security Center Web Console на устройство администратора;
- установка Агента администрирования и приложения безопасности на устройства организации.

В этом разделе

Руководство по усилению защиты

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

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

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

Руководство по усилению защиты содержит следующую информацию:

- выбор схемы развертывания Сервера Администрирования;

- настройка безопасного подключения к Серверу Администрирования;
- настройка учетных записей для работы с Сервером администрирования;
- управление защитой Сервера администрирования;
- управление защитой клиентских устройств;
- настройка защиты управляемых приложений;
- обслуживание Сервера администрирования;
- передача информации в сторонние системы;
- рекомендации по безопасности сторонних информационных систем.

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. 40) и их взаимодействием между собой (см. стр. 77), а также со схемами трафика данных и использования портов (см. стр. 65).

На основании этой информации нужно сформировать архитектуру, определяющую (см. стр. 224):

- расположение Сервера администрирования и подключение к сети;
- организацию рабочих мест администраторов и способы подключения к Серверу администрирования;
- способ установки Агента администрирования и приложения 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. 22).

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. 93). 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. 124).

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. 42). Оставшийся порт используется Веб-сервером Kaspersky Security Center (8060) (см. стр. 53). 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. 195). 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. 174).

Безопасность взаимодействия с внешней СУБД

Если СУБД устанавливается на отдельном устройстве при установке Сервера администрирования (внешняя СУБД), рекомендуется настроить параметры безопасного взаимодействия и аутентификацию с этой СУБД. Для получения дополнительной информации о настройке SSL-аутентификации см. Аутентификация сервера PostgreSQL и Сценарий: аутентификация сервера MySQL (см. стр. 221).

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. 500) 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 для аутентификации 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 для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования. Например, вы можете установить приложение для аутентификации 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. 493):

- Длина пароля должна быть от 8 до 256 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. 510).

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. 274). Предоставьте этой группе особые права доступа и создайте политику безопасности для нее (см. стр. 488).

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 приложения

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Сервера администрирования (см. стр. 478).

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. 608).

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

Отдельная учетная запись для удаленной установки приложений

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

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений. Вы можете назначить роль (см. стр. 494) или разрешения отдельной учетной записи (см. стр. 489).

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 приложения защиты Сервера администрирования

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

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

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

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

Создание отдельной политики безопасности для защиты приложения

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

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

Модули защиты

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

Настройка сетевого экрана устройства с Сервером администрирования

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

По умолчанию Сервер администрирования использует порт 13299 для приема подключения от Kaspersky Security Center Web Console (см. стр. 42). 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. 53).

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 управляемого приложения, и добавлять код активации или файл ключа на устройства вручную (см. стр. 379).

Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования (см. стр. 276).

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 приложений сторонних производителей и приложений "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. 290).

При необходимости вы также можете просмотреть Отчет о работе точек распространения (см. стр. 478).

Настройка защиты управляемых приложений

Политики управляемых приложений

Рекомендуется создать политику для каждого вида используемого приложения и компонента Kaspersky Security Center (Агент администрирования, Kaspersky Endpoint Security для Windows, Kaspersky Endpoint Security для Linux, Kaspersky Endpoint Agent и другие) (см. стр. 57). 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 приложения

Настоятельно рекомендуется включить защиту паролем, чтобы злоумышленники не смогли выключить или удалить приложения безопасности "Лаборатории Касперского". На платформах, где поддерживается защита паролем, вы можете установить пароль, например, для Kaspersky Endpoint Security, Агента администрирования и других приложений "Лаборатории Касперского" (см. стр. 425). После

включения защиты паролем рекомендуется заблокировать соответствующие параметры, закрыв их "замком".

Указание пароля для ручного подключения клиентского устройства к Серверу администрирования (утилита klmover)

Утилита klmover позволяет вручную подключить клиентское устройство к Серверу администрирования. При установке на клиентское устройство Агента администрирования утилита автоматически копируется в папку установки Агента администрирования.

Чтобы злоумышленники не могли вывести устройства из-под контроля вашего Сервера администрирования, настоятельно рекомендуется включить защиту паролем для запуска утилиты klmover. Чтобы включить защиту паролем, в параметрах политики Агента администрирования выберите параметр **Использовать пароль для удаления** (см. стр. 425).

Утилита klmover требует прав локального администратора. Защиту паролем для запуска утилиты klmover можно не устанавливать для устройств, работающих без прав локального администратора.

При включении параметра **Использовать пароль для удаления** также включается защита паролем средства удаления Kaspersky Security Center Web Console (cleaner.exe).

Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Сервера администрирования рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN (см. стр. 445). 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 (см. стр. 271).

Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с контроллерами доменов и указать диапазоны IP-адресов для обнаружения новых устройств (198).

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. 190). 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 приложения (см. стр. 193). Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи. Во время обслуживания Сервера администрирования приложение 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. 544).

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. 622).

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. 608) о публикуемых им событиях аудита (см. стр. 583), критических событиях (см. стр. 570), событиях отказа функционирования (см. стр. 572) и предупреждениях (см. стр. 575).

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

kaspersky

Сценарий: аутентификация MySQL Server

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

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

Включение односторонней SSL-аутентификации

Выполните следующие шаги, чтобы настроить одностороннюю SSL-аутентификацию для MySQL:

1. Создание самоподписанного сертификата SSL или TLS для SQL Server в соответствии с требованиями сертификата https://learn.microsoft.com/ru-ru/sql/linux/sql-server-linux-encrypted-connections?view=sql-server-ver16&tabs=client#requirements-for-certificates.

   Если у вас уже есть сертификат для SQL Server, пропустите этот шаг.

   SSL-сертификат можно применять только к версиям SQL Server ранее 2016 года (13.x). В версиях SQL Server 2016 (13.x) и выше используйте TLS-сертификат.

   o. **Создайте файл флага сервера**

   Перейдите в директорию ServerFlags и создайте файл, соответствующий флагу сервера KLSRV_MYSQL_OPT_SSL_CA:

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   touch KLSRV_MYSQL_OPT_SSL_CA
   ```

   p. **Измените файл флага сервера**

   В поле KLSRV_MYSQL_OPT_SSL_CA укажите путь к сертификату (файл ca-cert.pem).

   q. **Настройте базу данных**

   Укажите сертификаты в файле my.cnf. Откройте файл my.cnf в текстовом редакторе и добавьте следующие строки в раздел [mysqld]:

   ```
   [mysqld]
   ssl-ca="C:\mysqlCerts\ca-cert.pem"
   ssl-cert="C:\mysqlCerts\server-cert.pem"
   ssl-key="C:\mysqlCerts\server-key.pem"
   ```

Включение двусторонней SSL-аутентификации

Выполните следующие шаги, чтобы настроить двустороннюю SSL-аутентификацию для MySQL:

1. Создайте файлы флага сервера

   Перейдите в директорию ServerFlags и создайте файлы, соответствующие флагам сервера:

   ```
   cd /etc/opt/kaspersky/klnagent_srv/1093/1.0.0.0/ServerFlags/
   touch KLSRV_MYSQL_OPT_SSL_CA
   touch KLSRV_MYSQL_OPT_SSL_CERT
   ```

```
touch KLSRV_MYSQL_OPT_SSL_KEY
```

r. **Измените файлы флага сервера**

Изменить созданные файлы следующим образом:

KLSRV_MYSQL_OPT_SSL_CA: укажите путь к файлу ca-cert.pem.

KLSRV_MYSQL_OPT_SSL_CERT: укажите путь к файлу server-cert.pem.

KLSRV_MYSQL_OPT_SSL_KEY: укажите путь к файлу server-key.pem.

Если для server-key.pem требуется кодовая фраза, создайте файл KLSRV_MARIADB_OPT_TLS_PASPHRASE в папке ServerFlags и укажите в нем кодовую фразу.

s. **Настройте базу данных**

Укажите сертификаты в файле my.cnf. Откройте файл my.cnf в текстовом редакторе и добавьте следующие строки в раздел [mysqld]:

```
[mysqld]
ssl-ca="C:\mysqlCerts\ca-cert.pem"
ssl-cert="C:\mysqlCerts\server-cert.pem"
ssl-key="C:\mysqlCerts\server-key.pem"
```

Сценарий: аутентификация PostgreSQL Server

Рекомендуется использовать TLS-сертификат для аутентификации сервера PostgreSQL. Вы можете использовать сертификат доверенного центра сертификации (CA) или самоподписанный сертификат. Рекомендуется использовать сертификат доверенного 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
   ```

t. **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
```

u. **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`.

v. **Укажите сертификат PostgreSQL.**

Односторонняя SSL-аутентификация

Двусторонняя SSL-аутентификация

w. **Перезапустите демон PostgreSQL.**

Выполните следующую команду:

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

x. **Укажите флаг сервера для Сервера администрирования.**

Односторонняя SSL-аутентификация

Двусторонняя SSL-аутентификация

y. **Перезапустите службу Сервера администрирования.**

kaspersky

Подготовка к развертыванию

В этом разделе описаны шаги, которые вам нужно 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

kaspersky

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 приложения 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 с помощью Kaspersky Security Center Web Console.

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

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

  Установка приложений "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. 234)). 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. 228).

В разделе "Типовые конфигурации Kaspersky Security Center" приведены подробные описания типовых конфигураций Kaspersky Security Center (см. стр. 227). 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 286

Типовая конфигурация: несколько крупных офисов с собственными администраторами 228

Типовая конфигурация: множество небольших удаленных офисов 228

Начало работы 87

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 87

В этом разделе

Типовая конфигурация: один офис 228

Типовая конфигурация: несколько крупных офисов с собственными администраторами 228

Типовая конфигурация: множество небольших удаленных офисов 228

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 233

Порты, используемые Kaspersky Security Center 42

Начало работы 87

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. 228). 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 228

Порты, используемые Kaspersky Security Center 42

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. 295).

См. также:

О точках распространения 233

Предоставление доступа к Серверу администрирования из интернета 230

Порты, используемые Kaspersky Security Center 42

Выбор СУБД

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

Таблица 22. Рекомендации и ограничения СУБД

СУБД	Рекомендации и ограничения
MySQL (см. поддерживаемые версии на стр. 22)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах.
MariaDB (см. поддерживаемые версии на стр. 22)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 20 000 устройствах.
PostgreSQL, Postgres Pro (см. поддерживаемые версии на стр. 22)	Используйте эту СУБД, если вы планируете запустить один Сервер администрирования менее чем на 50 000 устройствах.

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 приложений.

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. 91), PostgreSQL (см. стр. 93) или Postgres Pro (см. стр. 93) используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

См. также:

Учетные записи для работы с СУБД 124

Начало работы 87

Предоставление доступа к Серверу администрирования из интернета

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

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

  По умолчанию Сервер администрирования не требует подключения к интернету для установки обновлений приложений Microsoft на управляемые устройства. Например, управляемые устройства могут загружать обновления приложений 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 приложений сторонних производителей, отличных от приложений Microsoft.
- Закрытие уязвимостей в приложениях сторонних производителей

  Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:

  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений 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.

См. также:

Начало работы 87

В этом разделе

Доступ из интернета: 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:

Порты, используемые Kaspersky Security Center 42
Начало работы 87
Схемы трафика данных и использования портов 65

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 приложения 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. 233).

См. также:

Сервер администрирования внутри демилитаризованной зоны (DMZ), управляемые устройства в интернете.....74

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. 63). В этом случае для организации доступа из интернета нужно выполнить следующие условия:

- На устройство, находящееся в демилитаризованной зоне, следует установить Агент администрирования (см. стр. 262). 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.

kaspersky

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. 541).

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. 295).

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 285
Начало работы 87

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 23. 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 24. 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 25. 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 26. 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 приложений "Лаборатории Касперского".....515

Типовая конфигурация: множество небольших удаленных офисов.....228

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 приложений 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 27. Сетевые параметры

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Активация приложения.
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 приложений "Лаборатории Касперского" (см. стр. 518).
Порт: 443 Протокол: HTTPS	https://downloads.upd.kaspersky.com	• Обновление баз и приложений "Лаборатории Касперского" (см. стр. 518). • 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, приложение использует публичные DNS-серверы (см. стр. 194).

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 приложений "Лаборатории Касперского" (см. стр. 518).

Сетевые параметры	Адрес	Описание
Порт: 443 Протокол: HTTPS	ds.kaspersky.com	Использование Kaspersky Security Network (см. стр. 445).
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. 445).
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	Серверы для проверки сертификатов, необходимых для настройки TLS-соединения с другими серверами "Лаборатории Касперского".
Порт: 443 Протокол: HTTPS	https://ipm-klca.kaspersky.com	Рекламные объявления (см. стр. 615).

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).

► *Чтобы загрузить обновления по протоколу HTTP или HTTPS с помощью утилиты klscflag:*

1. Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
2. Если вы хотите загружать обновления (см. стр. 518) по протоколу HTTP, выполните одну из следующих команд под учетной записью root:
   - На устройстве, на котором установлен Сервер 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 (см. стр. 518) по протоколу HTTPS, выполните одну из следующих команд под учетной записью root:

- На устройстве, на котором установлен Сервер 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
  ```

Развертывание Агента администрирования и приложения безопасности

Для управления устройствами организации требуется установить на устройства Агент администрирования. Развертывание распределенного приложения Kaspersky Security Center на устройствах организации обычно начинается с установки на них Агента администрирования.

В Microsoft Windows XP Агент администрирования может некорректно выполнять следующие операции: загружать обновления непосредственно с серверов "Лаборатории Касперского" (в качестве точки распространения) и работать в качестве прокси-сервера KSN (в качестве точки распространения).

В этом разделе

Первоначальное развертывание

Если на устройстве уже установлен Агент администрирования, удаленная установка приложений на такое устройство осуществляется с помощью самого Агента администрирования. При этом передача дистрибутива устанавливаемого приложения 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 приложений 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 приложений.
- 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 приложений Kaspersky Security Center.
- Принудительно с помощью соответствующих параметров в задаче удаленной установки приложений 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 приложений с настроенными параметрами.
- Вручную, запуская инсталляторы приложений 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 приложения "Лаборатории Касперского" на этих платформах можно с помощью задач удаленной установки приложений, используя уже имеющиеся на устройствах Агенты администрирования. Установка в этом случае происходит аналогично установке на платформе Microsoft Windows.

Выбирая способ и стратегию развертывания приложений в управляемой сети, следует принимать во внимание ряд факторов (неполный список):

- конфигурация сети организации (см. стр. 227);
- общего количества устройств;
- наличие в сети организации устройств, не являющихся членами доменов Active Directory, и наличие унифицированных учетных записей с административными правами на таких устройствах;
- ширину канала между Сервером администрирования и устройствами;
- тип связи между Сервером администрирования и удаленными подсетями и ширину сетевых каналов внутри таких подсетей;
- используемые на момент начала развертывания параметры безопасности на удаленных устройствах (в частности использование UAC и режима Simple File Sharing).

kaspersky

В этом разделе

Настройка параметров инсталляторов

Прежде чем приступать к развертыванию в сети приложений "Лаборатории Касперского", следует определить параметры инсталляции – те параметры, которые настраиваются в ходе установки приложения. 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 приложений 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 приложений является универсальным и подходит для всех способов установки приложений: как средствами Kaspersky Security Center, так и с помощью большинства сторонних средств. Этот способ подразумевает создание в Kaspersky Security Center инсталляционных пакетов приложений.

Инсталляционные пакеты создаются следующими способами:

- автоматически из указанных дистрибутивов на основании входящих в их состав *описателей* (файлов с расширением kud, содержащих правила установки и анализа результата и другую информацию);
- из исполняемых файлов инсталляторов или инсталляторов в собственном формате (.msi, .deb, .rpm) – для стандартных или поддерживаемых приложений.

Созданные инсталляционные пакеты представляют собой папки с вложенными подпапками и файлами. Помимо исходного дистрибутива, в состав инсталляционного пакета входят редактируемые параметры (включая параметры самого инсталлятора и правила обработки таких ситуаций, как необходимость перезагрузки операционной системы для завершения инсталляции), а также небольшие вспомогательные модули.

Значения параметров установки, специфичные для конкретного поддерживаемого приложения, можно задавать в пользовательском интерфейсе Kaspersky Security Center Web Console при создании инсталляционного пакета. В случае удаленной установки приложений средствами Kaspersky Security Center

инсталляционные пакеты доставляются на устройства таким образом, что при запуске инсталлятора приложения ему становятся доступны все заданные администратором параметры. При использовании сторонних средств установки приложений "Лаборатории Касперского" достаточно обеспечить доступность на устройстве всего инсталляционного пакета, то есть дистрибутива и его параметров. Инсталляционные пакеты создаются и хранятся Kaspersky Security Center в соответствующей подпапке папки общего доступа (см. стр. 139).

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 приложения безопасности для платформы Microsoft Windows.

Несмотря на то, что лицензионный ключ для лицензии на приложение 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 приложений Kaspersky Security Center

Kaspersky Security Center предоставляет разнообразные механизмы удаленной установки приложений, реализованные в виде задач удаленной установки приложений (принудительная установка, установка с помощью копирования образа жесткого диска). Создать задачу удаленной установки можно как для указанной группы администрирования, так и для набора устройств или для выборки устройств (такие задачи отображаются в Kaspersky Security Center Web Console в папке **Задачи**). При создании задачи можно выбрать инсталляционные пакеты (Агента администрирования и/или другого приложения), подлежащие установке при помощи данной задачи, а также задать ряд параметров, определяющих способ удаленной установки. Кроме того, можно воспользоваться мастером удаленной установки приложений, в основе которого также лежит создание задачи удаленной установки приложений и мониторинг результатов.

Задачи для групп администрирования действуют не только на устройства, принадлежащие этой группе, но и на все устройства всех подгрупп выбранной группы. Если в параметрах задачи включен соответствующий параметр, задача распространяется на устройства подчиненных Серверов администрирования, расположенных в данной группе или ее подгруппах.

Задачи для наборов устройств актуализируют список клиентских устройств при каждом запуске в соответствии с составом выборки устройств на момент запуска задачи. Если в выборке устройств присутствуют устройства, подключенные к подчиненным Серверам администрирования, задача будет запускаться и на этих устройствах. Подробнее об этих параметрах и способах установки будет рассказано далее в этом разделе.

Для успешной работы задачи удаленной установки на устройствах, подключенных к подчиненным Серверам администрирования, следует при помощи задачи ретрансляции предварительно ретранслировать используемые задачей инсталляционные пакеты на соответствующие подчиненные Серверы администрирования.

Развертывание захватом и копированием образа устройства

Если нужно инсталлировать Агент администрирования на устройства, на которые также предстоит установить (или переустановить) операционную систему и прочее программное обеспечение, можно воспользоваться механизмом захвата и копирования образа устройства.

► *Чтобы выполнить развертывание путем захвата и копирования жесткого диска:*

1. Создать эталонное устройство с установленной операционной системой и необходимым для работы набором программного обеспечения, включая Агент администрирования и приложение 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. 244).

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 244

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 Kaspersky Security Center Web Console как одно устройство. Проблема возникает потому, что при клонировании на новых устройствах сохраняются одинаковые внутренние данные, позволяющие Серверу администрирования связать устройство со своей записью в Kaspersky Security Center Web Console.

Избежать проблемы с неверным отображением новых устройств в Kaspersky Security Center Web Console 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 одной записью в Kaspersky Security Center Web Console. По завершении клонирования образа эталонного устройства, новые устройства отображаются в Kaspersky Security Center Web Console нормально (как отдельные записи).

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 243

Принудительное развертывание с помощью задачи удаленной установки приложений Kaspersky Security Center

В случае если требуется начать развертывание Агентов администрирования или других необходимых приложений 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, которая описана на веб-сайте Службы технической поддержки "Лаборатории Касперского".

При установке на новые устройства, еще не размещенные в группах администрирования Kaspersky Security Center, в свойствах задачи удаленной установки можно задать группу администрирования, в которую устройства будут перемещаться по завершении установки на них Агента администрирования.

При создании групповой задачи необходимо помнить, что групповая задача действует на устройства всех вложенных подгрупп выбранной группы. Поэтому не следует дублировать задачи установки в подгруппах.

Можно использовать упрощенный способ создания задач принудительной установки приложений – автоматическую установку. Для этого в свойствах группы администрирования нужно выбрать в списке инсталляционных пакетов те пакеты, которые должны быть установлены на устройствах этой группы. В результате на всех устройствах этой группы и ее подгрупп будут автоматически установлены выбранные инсталляционные пакеты. Период, в течение которого будут установлены пакеты, зависит от пропускной способности сети и общего количества устройств в сети.

Принудительная установка может быть использована и в случае, если устройства не доступны Серверу администрирования непосредственно: например, устройства расположены в изолированных сетях, или устройства расположены в локальной сети, а Сервер администрирования – в демилитаризованной зоне. Для работоспособности принудительной установки необходимо обеспечить наличие точек распространения в каждой такой изолированной сети.

Использование точек распространения в качестве локальных центров установки может быть удобно и для установки на устройства в подсетях, соединенных с Сервером администрирования узким каналом связи при наличии широкого канала связи между устройствами внутри подсети. Однако следует учитывать, что данный способ установки создает значительную нагрузку на устройства, назначенные точками распространения. Поэтому нужно выбирать в качестве точек распространения мощные устройства с высокопроизводительными накопителями. Также необходимо, чтобы объем свободного места в разделе с папкой /var/opt/kaspersky/klnagent_srv/ многократно превосходил суммарный объем дистрибутивов устанавливаемых приложений.

Запуск автономных пакетов, сформированных Kaspersky Security Center

Описанные выше способы первоначального развертывания Агента администрирования и приложений могут быть реализованы не всегда из-за невозможности выполнить все необходимые условия. В таких случаях из подготовленных администратором инсталляционных пакетов с необходимыми параметрами установки средствами Kaspersky Security Center можно создать единый исполняемый файл, который называется *автономным пакетом установки*. Автономный инсталляционный пакет может быть опубликован как на внутреннем Веб-сервере (входящем в состав Kaspersky Security Center), если это имеет смысл (настроен доступ к этому Веб-серверу извне для пользователей устройств), так и на специально развернутом Веб-сервере, входящем в состав Kaspersky Security Center Web Console. Также можно скопировать автономные пакеты на другой Веб-сервер.

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 Веб-серверу. Администратор может скопировать автономный пакет на съемный диск и доставить пакет на нужное устройство с целью его последующего запуска.

Автономный пакет можно создать из пакета Агента администрирования, пакета другого приложения (например, приложения безопасности) или сразу из обоих пакетов. Если автономный пакет создан из Агента администрирования и другого приложения, установка начнется с Агента администрирования.

При создании автономного пакета с Агентом администрирования можно указать группу администрирования, в которую будут автоматически перемещаться новые устройства (ранее не размещенные в группах администрирования) по завершении установки на них Агента администрирования.

Автономные пакеты могут работать интерактивно (по умолчанию), с отображением результата установки входящих в них приложений, или в "тихом" режиме (при запуске с ключом "-s"). "Тихий" режим может быть использован для установки из каких-либо скриптов (например, из скриптов, настраиваемых для запуска по завершении развертывания образа операционной системы, и тому подобное). Результат установки в тихом режиме определяется кодом возврата процесса.

Удаленная установка приложений на устройства с установленным Агентом администрирования

Если на устройстве установлен работоспособный Агент администрирования, подключенный к главному Серверу администрирования или к одному из его подчиненных Серверов, то на этом устройстве можно обновлять версию Агента администрирования, а также устанавливать, обновлять или удалять с помощью Агента администрирования любые поддерживаемые приложения.

Эта функция включается параметром **Использовать Агент администрирования** в свойствах задачи удаленной установки приложений (см. стр. 242).

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. разделы "О точках распространения" (стр. 233)и "Построение структуры групп администрирования и назначение точек распространения" (стр. 285)). 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 приложений.

При передаче инсталляционных пакетов на устройства по каналам связи между Агентами администрирования и Сервером администрирования подготовленные к передаче инсталляционные пакеты дополнительно кешируются в папке /var/opt/kaspersky/klnagent_srv/1093/.working/. 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 невозможно. При удалении исходных инсталляционных пакетов соответствующие данные будут автоматически удаляться и из папки FTServer.

Данные, принимаемые точками распространения, сохраняются в папке /var/opt/kaspersky/klnagent_srv/1103/.

Удалять файлы из папки $FTCITmp вручную невозможно. 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, невозможно 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 Kaspersky Security Center Web Console. Изменение параметров инсталляционного пакета в Kaspersky Security Center Web Console заставит Сервер администрирования обновить образ пакета в кеше, подготовленном для передачи на устройства.

Сервер отправляет эхо-запросы ICMP (такие же, как и команда ping) на целевое устройство во время удаленной установки.

Управление перезагрузкой устройств в задаче удаленной установки

Часто для завершения удаленной установки приложений (особенно на платформе Windows) требуется перезагрузка устройства.

Если используется задача удаленной установки приложений 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.

kaspersky

Целесообразность обновления баз в инсталляционном пакете приложения безопасности

Перед началом развертывания защиты необходимо учитывать возможность обновления антивирусных баз (включая модули автопатчей), распространяемых вместе с дистрибутивом приложения безопасности. Целесообразно перед началом развертывания принудительно обновить базы в составе инсталляционного пакета приложения (например, с помощью соответствующей команды в контекстном меню выбранного инсталляционного пакета). Это уменьшит количество перезагрузок, требующихся для завершения развертывания защиты на устройствах.

Мониторинг развертывания

Чтобы контролировать развертывание Kaspersky Security Center и убедиться, что приложение безопасности и Агент администрирования установлены на управляемых устройствах, используйте функции мониторинга и отчеты (см. стр. 544):

- Используйте веб-виджет развертывания в панели инструментов для мониторинга развертывания в режиме реального времени (см. стр. 551).
- Используйте отчеты, чтобы получить подробную информацию (см. стр. 556).

Настройка параметров инсталляторов

В разделе содержится информация о файлах инсталляторов Kaspersky Security Center и параметрах установки, а также рекомендации по установке Сервера администрирования и Агента администрирования в "тихом" режиме.

В этом разделе

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.

kaspersky

См. также:

Установка в тихом режиме (с файлом ответов)

В инсталляторе 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 приложение 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 Kaspersky Security Center Web Console.

См. также:

Частичная настройка параметров установки через setup.exe

Запуская установку приложений через setup.exe, можно передавать в MSI-пакет значения любых свойств MSI.

Команда будет выглядеть следующим образом:

Пример:

```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

См. также:

Параметры установки Сервера администрирования

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

Таблица 28. 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

Имя переменной	Обязательная	Описание	Возможные значения
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

Имя переменной	Обязательная	Описание	Возможные значения
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

Имя переменной	Обязательная	Описание	Возможные значения
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. 112), 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 KLFOC_UNATT_CONN_MODE имеет значение VirtualAdapter, файл ответов должен включать следующие дополнительные переменные:

Имя переменной	Обязательная	Описание	Возможные значения
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 29. 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. 368). • 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. В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.	• 1 – использовать; • другое значение или не задано – не использовать.

Свойство MSI	Описание	Доступные значения
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Адрес прокси-сервера и номер порта для подключения к прокси-серверу.	Строковое значение.
PROXYLOGIN	Учетная запись для подключения к прокси-серверу.	Строковое значение.
PROXYPASSWORD	Пароль учетной записи для подключения к прокси-серверу (указывайте в параметрах инсталляционных пакетов данные привилегированных учетных записей).	Строковое значение.
GATEWAYMODE	Режим использования шлюза соединения.	• 0 – не использовать шлюз соединений; • 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.

kaspersky

См. также:

Виртуальная инфраструктура

Kaspersky Security Center поддерживает работу с виртуальными машинами. Вы можете установить Агент администрирования и приложения 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 обычное приложение 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. 260).

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 Kaspersky Security Center Web Console.

См. также:

Начало работы 87

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. 267);
- 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 87

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. 243).

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 87

Поддержка отката файловой системы для устройств с Агентом администрирования

Kaspersky Security Center является распределенным приложением. 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 приложений

В этом разделе описана процедура установки приложений, которые могут быть установлены на устройства только локально.

Для проведения локальной установки приложений на выбранном клиентском устройстве вам необходимо обладать правами администратора на этом устройстве.

► *Чтобы установить приложения 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 приложения согласно описаниям, изложенным в Руководствах к этим приложениям.
3. Установите на рабочее место администратора плагин управления для каждого из установленных приложений.

Kaspersky Security Center также поддерживает возможность локальной установки приложений с помощью автономного инсталляционного пакета. Kaspersky Security Center не поддерживает установку всех приложений «Лаборатории Касперского».

В этом разделе

См. также:

Начало работы 87

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 приложений "Лаборатории Касперского" для установки.

2. В окне с выбором приложений 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 для VM**.

      В результате будет выключена проверка исполняемых файлов на наличие уязвимостей при запуске устройства. Также будет выключена передача на Сервер администрирования следующей информации:

      - о реестре оборудования;
      - о приложениях, установленных на устройстве;
      - об обновлениях Microsoft Windows, которые необходимо установить на локальном клиентском устройстве;
      - об уязвимостях в приложениях, 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, а также запускать, останавливать и контролировать активность Агента администрирования с помощью стандартных инструментов Microsoft Windows: Управление компьютером\Службы.

См. также:

Поддержка динамических виртуальных машин 259

Просмотр Политики конфиденциальности 370

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 приложения Kaspersky Security Center в папке Packages\NetAgent\exec.

► *Чтобы установить Агент администрирования на локальном устройстве в тихом режиме:*

1. Прочитайте Лицензионное соглашение (см. стр. 368). 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 вам нужно включить параметр `EULA=1`. В противном случае Агент администрирования не будет установлен.

Если вы используете стандартные параметры подключения для Kaspersky Security Center 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, приложение создает файл $klssinstlib.log, который содержит журнал событий установки. Этот файл хранится в папке %windir%\temp or %temp%. Для устранения неполадок вам или специалисту Службы технической поддержки "Лаборатории Касперского" могут потребоваться оба файла журнала – nag_inst.log и $klssinstlib.log.

Если вам необходимо дополнительно указать порт для подключения к Серверу администрирования, введите команду:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx
c:\windows\temp\nag_inst.log SERVERADDRESS=kscserver.mycompany.com
EULA=1 SERVERPORT=14000
```

Параметр `SERVERPORT` соответствует номеру порта подключения к Серверу администрирования.

Имена и возможные значения параметров, которые можно использовать при установке Агента администрирования в тихом режиме, приведены в разделе Параметры установки Агента администрирования (см. стр. 255).

См. также:

Параметры установки Агента администрирования 255
Параметры установки Сервера администрирования 251
Просмотр Политики конфиденциальности 370

Локальная установка плагина управления приложением

► *Чтобы установить плагин управления приложением,*

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

Файл klcfginst.exe входит в состав всех приложений, которыми может управлять Kaspersky Security Center. Установка сопровождается мастером и не требует настройки параметров.

Установка приложений в тихом режиме

► *Чтобы установить приложение в тихом режиме:*

1. Откройте главное окно приложения Kaspersky Security Center.
2. В папке дерева консоли **Удаленная установка** во вложенной папке **Инсталляционные пакеты** выберите инсталляционный пакет нужного приложения или сформируйте для этого приложения 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 выбранного приложения 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 приложений "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. 368) и Политики конфиденциальности соответственно (см. стр. 370). 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 приложения или обновления предыдущей версии приложения.

Установка программ с помощью автономных пакетов

Kaspersky Security Center позволяет формировать автономные инсталляционные пакеты приложений. 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 приложения без участия Kaspersky Security Center.

► *Чтобы установить приложение 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 нужного приложения.
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 приложения на клиентское устройство.
6. Запустите автономный инсталляционный пакет на клиентском устройстве.

В результате приложение будет установлено на клиентском устройстве с параметрами, указанными в автономном пакете.

При создании автономный инсталляционный пакет автоматически публикуется на Веб-сервере. Ссылка для загрузки автономного пакета отображается в списке созданных автономных инсталляционных пакетов. При необходимости вы можете отменить публикацию выбранного автономного пакета и снова опубликовать его на Веб-сервере. По умолчанию для загрузки автономных инсталляционных пакетов используется порт 8060.

Параметры инсталляционного пакета Агента администрирования

► *Чтобы настроить параметры инсталляционного пакета Агента администрирования:*

1. В дереве консоли в папке **Удаленная установка** выберите вложенную папку **Инсталляционные пакеты**.

   Папка **Удаленная установка** по умолчанию вложена в папку **Дополнительно**.

2. В контекстном меню инсталляционного пакета Агента администрирования выберите пункт **Свойства**.

Откроется окно свойств инсталляционного пакета Агента администрирования.

Общие

Раздел **Общие** содержит общую информацию об инсталляционном пакете:

- название инсталляционного пакета;
- имя и версию приложения, для которого 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 приложения (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 со статусом "Не определено".**

  Если этот параметр включен, все загруженные обновления и патчи для Сервера администрирования, Агента администрирования, Kaspersky Security Center Web Console, 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. 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.

- **Использовать сертификат Сервера**

  Если этот параметр включен, для аутентификации доступа Агента администрирования к Серверу администрирования будет использоваться файл сертификата, который можно указать при нажатии на кнопку **Обзор**.

  Если этот параметр выключен, файл сертификата будет получен с Сервера администрирования при первом подключении Агента администрирования по адресу, указанному в поле **Адрес сервера**.

  Не рекомендуется выключать параметр, так как автоматическое получение сертификата Сервера администрирования Агентом администрирования при подключении к Серверу является небезопасным.

  По умолчанию флажок установлен.

- **Использовать SSL-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.

- **Использовать прокси-сервер**

В целях совместимости не рекомендуется указывать параметры подключения к прокси-серверу в параметрах инсталляционного пакета Агента администрирования.

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. 63).
- Подключайтесь к Серверу администрирования с помощью шлюза соединения, чтобы уменьшить количество подключений к Серверу администрирования. В этом случае введите адрес устройства, которое будет выступать в качестве шлюза соединения в поле **Адрес шлюза соединения**.
- Настройте подключение для Virtual Desktop Infrastructure (VDI), если в вашей сети есть виртуальные машины. Для этого выполните следующее:
  - **Включить динамический режим для VDI**

    Если параметр включен, для Агента администрирования, установленного на виртуальной машине, будет включен динамический режим для Virtual Desktop Infrastructure (VDI).

    По умолчанию параметр выключен.

  - **Оптимизировать параметры для VDI**

    Если параметр включен, в параметрах Агента администрирования выключены

следующие функции:

- получение информации об установленном программном обеспечении;
- получение информации об аппаратном обеспечении;
- получение информации о наличии уязвимостей;
- получение информации о необходимых обновлениях.

По умолчанию параметр выключен.

Дополнительные компоненты

В этом разделе можно выбрать дополнительные компоненты для совместной установки с Агентом администрирования.

Теги

В разделе **Теги** отображается список ключевых слов (тегов), которые можно добавлять клиентским устройствам после установки на них Агента администрирования. Вы можете добавлять и удалять теги из списка, а также переименовывать теги.

Если рядом с тегом установлен флажок, тег будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования.

Если флажок рядом с тегом снят, тег не будет автоматически добавлен управляемым устройствам при установке на них Агента администрирования. Этот тег можно добавить устройствам вручную.

При удалении тега из списка тег автоматически снимается со всех устройств, которым он добавлен.

История ревизий

В этом разделе можно посмотреть историю ревизий инсталляционного пакета (см. стр. 634). 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 30. 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**)

Раздел свойств	Windows	Mac	Linux
Дополнительно	✓	✓	✓
Дополнительные компоненты	✓	✓	✓
Теги	✓	✓ (кроме правил автоматического назначения тегов)	✓ (кроме правил автоматического назначения тегов)
История ревизий	✓	✓	✓

Веб-сервер Kaspersky Security Center

Веб-сервер Kaspersky Security Center (далее Веб-сервер) – это компонент Kaspersky Security Center. Веб-сервер используется для публикации автономных инсталляционных пакетов и файлов из папки общего доступа.

Созданные инсталляционные пакеты публикуются на Веб-сервере автоматически и удаляются после первой загрузки. Администратор может передать сформированную ссылку пользователю любым удобным способом, например, по электронной почте.

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

Настройка Веб-сервера

Для тонкой настройки Веб-сервера в свойствах Веб-сервера можно сменить порты для протоколов HTTP (8060) и HTTPS (8061). Также, помимо смены портов, возможна смена серверного сертификата для HTTPS-протокола и смена FQDN-имени веб-сервера для HTTP-протокола.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства (см. стр. 143). Если автоматически заданное расписание задачи групповой проверки не подходит для вашей организации, вам нужно вручную настроить наиболее удобное расписание для этой задачи на основе правил рабочего процесса, принятых в организации.

Например, для задачи выбрано расписание **Запускать по пятницам в 19:00** с автоматической рандомизацией и снят флажок **Запускать пропущенные задачи**. Это означает, что если устройства организации выключаются по пятницам, например, в 18:30, то задача проверки устройства никогда не будет запущена. В этом случае вам необходимо настроить задачу групповой проверки вручную.

kaspersky

См. также:

Сценарий: настройка защиты сети.....393

kaspersky

Управление клиентскими устройствами

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

В этом разделе

См. также:

Сценарий: настройка защиты сети 393

Параметры управляемого устройства

► *Чтобы просмотреть параметры управляемого устройства:*

1. В главном окне приложения 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.

В верхней части окна свойств отображаются следующие вкладки, на которых представлены основные группы параметров:

- **Общие**
- **Приложения**
- **Активные политики и профили политик**
- **Задачи**
- **События**
- **Проблемы безопасности**
- **Теги**
- **Дополнительно**

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).

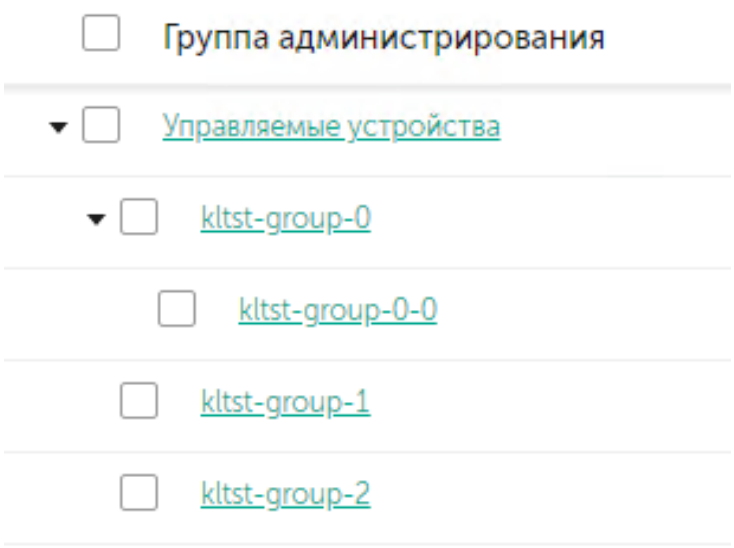


Рисунок 1. Просмотр иерархии групп администрирования

► *Чтобы создать группу администрирования:*

1. В главном окне приложения 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 приложения 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. 279). 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 приложения* 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. 58), назначать Агенты администрирования согласно методике (см. стр. 285) и так далее.

См. также:

Начало работы 87

Создание правил перемещения устройств

Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования (см. стр. 276).

► *Чтобы создать правило перемещения устройств:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне укажите следующие данные на вкладке **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 вкладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования (см. стр. 279).
5. Нажмите на кнопку **Сохранить**.

Правило перемещения создано. 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 выбран параметр **Применять правило постоянно**, правило перемещения применяется независимо от приоритета. Такие правила применяются по расписанию, которое Сервер администрирования устанавливает автоматически.

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 281

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 приложения перейдите в раздел **Активы (Устройства)** → **Правила перемещения**.
- В главном окне приложения 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 вкладке **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. 279).
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. 276) или копировании (см. стр. 277) правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств (см. стр. 276). 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 приложения, 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. 318). Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

- **Применить к устройствам без выбранных тегов**
- **Применить, 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**
- **IP-диапазон**
- **IP-адрес подключения к Серверу**
- **Изменение профиля подключения**
- **Под управлением другого Сервера администрирования**

Вкладка Владелец устройства

На этой вкладке вы можете настроить правило перемещения устройств в зависимости от владельца устройств, членства в группе безопасности и ролей:

- **Владелец устройства**
- **Членство владельца устройства в группе безопасности Active Directory**
- **Роль владельца устройства**
- **Членство владельца устройства во внутренней группе безопасности**

Вкладка Приложения

На этой вкладке можно настроить правило перемещения устройств на основе управляемых приложений и операционных систем, установленных на клиентских устройствах:

- **Агент администрирования установлен**
- **Приложения**
- **Версия операционной системы**
- **Архитектура 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**

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 приложения 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 276

Перемещение устройств или кластеров в состав группы администрирования вручную 282

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. 283). 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.

О кластерах и массивах серверов

Kaspersky Security Center поддерживает кластерную технологию. Если Агент администрирования передает Серверу администрирования информацию о том, что приложение, установленное 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. 273). Вы можете удалить или переместить только весь кластер.

Вы можете выполнять следующие операции с кластерами или массивами серверов:

- Просмотр свойств (см. стр. 284)
- Переместить кластер или массив серверов в другую группу администрирования (см. стр. 282).

  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 приложение "Лаборатории Касперского" по-прежнему установлено на узлах кластера, Kaspersky Security Center автоматически возвращает удаленный кластер и его узлы обратно в список управляемых устройств.

См. также:

Свойства кластеров или массивов серверов 284

kaspersky

Свойства кластеров или массивов серверов

► *Чтобы просмотреть параметры кластера или массива серверов:*

1. В главном окне приложения 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:

- **Название**
- **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 приложению "Лаборатории Касперского", установленного 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. 273).

Приложений "Лаборатории Касперского"

Окно свойств также может содержать дополнительные вкладки с информацией и параметрами, относящимися к приложению "Лаборатории Касперского", установленного на узлах кластера.

См. также:

О кластерах и массивах серверов 283

kaspersky

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью *профилей политик*.

- Задание области действия групповых задач.

  Существует подход к заданию области действия групповых задач, не основанный на иерархии групп администрирования: использование задач для выборок устройств и наборов устройств.

- Задание прав доступа к устройствам, виртуальным и подчиненным Серверам администрирования.
- Назначение точек распространения.

При построении структуры групп администрирования следует учитывать топологию сети организации для оптимального назначения точек распространения. Оптимальное распределение точек распространения позволяет уменьшить сетевой трафик внутри сети организации.

В зависимости от организационной структуры организации и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- Один офис.
- Множество небольших изолированных офисов.

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

В этом разделе

См. также:

kaspersky

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 приложений "Лаборатории Касперского".....515

Типовая конфигурация точек распространения: множество небольших удаленных 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).

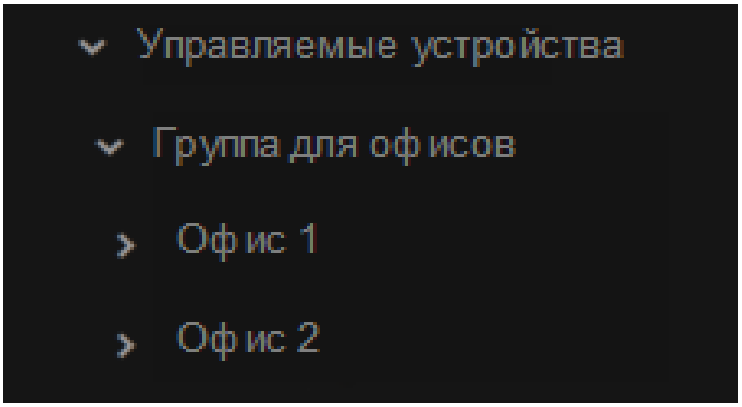


Рисунок 2. Удаленные офисы отражены в структуре групп администрирования

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 31. 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 32. 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 33. 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 34. 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 приложений "Лаборатории Касперского".....515

Типовая конфигурация: множество небольших удаленных офисов.....228

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 вкладке **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 приложений "Лаборатории Касперского" 515

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. 234).

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 вкладке **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 приложений из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке приложения 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. 234) 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. 234) количество точек распространения в вашей сети для оптимизации трафика и нагрузки.

Если вы выключите этот параметр, количество загрузок инсталляционных пакетов и нагрузка на Сервер администрирования могут увеличиться. По умолчанию параметр включен.

- **Запустить push-сервер**
- Порт push-сервера

- В разделе **Область действия** укажите 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. 539).

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 приложение 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 управляемого приложения 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**
  - **Использовать HTTPS**

    Если вам нужно, чтобы управляемые устройства подключались к прокси-серверу KSN через порт HTTPS, включите параметр **Использовать HTTPS** и укажите номер порта в поле **Через HTTPS-порт**. По умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.
  - **Через HTTPS-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, вам нужно 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.

kaspersky

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 приложения 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 приложения 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. 415) 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 управляемого приложения 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 вкладке **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 выбранной точке распространения.

См. также:

Принудительная синхронизация 415

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 35. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Не установлено приложение безопасности	Агент администрирования установлен на устройстве, но не установлено приложение 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 установлено приложение 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 установлено приложение 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 приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.

Условие	Описание условия	Доступные значения
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	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 приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
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.
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • 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.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• 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.

Условие	Описание условия	Доступные значения
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Не запущено приложение безопасности	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• 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. столбец "Описание условий" в таблице выше) 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 607

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 36. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Не установлено приложение безопасности	Агент администрирования установлен на устройстве, но не установлено приложение 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 установлено приложение 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 установлено приложение 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
Restart is required.	Устройство видимо в сети, но приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Флажок снят. • Флажок установлен.

Условие	Описание условия	Доступные значения
Обнаружены уязвимости в приложениях	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 приложениях 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.
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.

Условие	Описание условия	Доступные значения
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 приложением	Статус устройства определяется управляемым приложением.	• 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.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве выключено больше указанного времени.	Более чем 0 минут
Не запущено приложение безопасности	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• Флажок снят. • Флажок установлен.

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 невозможно 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 установленного приложения, то в выборку устройств попадут только те устройства, на которых одновременно установлено указанное приложение и их IP-адреса входят в указанный диапазон.

См. также:

Использование выборок событий 589

Сценарий: настройка защиты сети 393

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 приложения 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. 452).

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 приложения 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. 306), 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 приложения 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.

- **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"**.

- **IP-диапазон**

  Если этот параметр включен, в полях ввода можно указать начальный и конечный IP-адреса интервала, в который должны входить искомые устройства.

  По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

В разделе **Контроллеры доменов** можно настроить критерии включения устройств в выборку по членству в домене:

- **Устройство в подразделении домена**
- **Устройство является членом группы Active Directory**

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**. Приложение включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Приложение 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 управляемого приложения:

- **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 приложений** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых приложений:

- **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 антивирусной защиты серверов совместной работы (*Нет данных*, *Остановлена*, *Запускается, Приостановлена*, *Выполняется*, *Сбой*).

- **Статус антивирусной защиты почтовых серверов**

Поиск устройств по статусу антивирусной защиты почтовых серверов (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

- **Статус Endpoint Sensor**

Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных, Остановлена, Запускается, Приостановлена, Выполняется, Сбой*).

В разделе **Проблемы, связанные со статусом управляемых приложений** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемым приложением. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких приложений, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемого приложения, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких приложений, 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.

- **Архитектура 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.

- **Поставщик устройства**

  Название производителя устройства. Устройства, изготовленные производителем, указанным в поле, будут включены в состав выборки.

  Название производителя можно ввести в окне свойств устройства.

- **Серийный номер**

  Оборудование с серийным номером, указанным в поле, будет включено в выборку.

- **Инвентарный номер**

  Оборудование с инвентарным номером, указанным в поле, будет включено в выборку.

- **Пользователь**

  Оборудование пользователя, указанного в поле, будет включено в выборку.

- **Расположение**

  Место расположения устройства или оборудования (например, в офисе или филиале). Компьютеры или другие устройства с расположением, указанным в поле, будут включены в состав выборки.

Расположение оборудования в произвольной форме можно ввести в окне свойств оборудования.

- **Частота процессора (МГц) от**
- **Частота процессора (МГц) до**
- **Количество виртуальных ядер процессора от**

- **Количество виртуальных ядер процессора до**
- **Объем жесткого диска (ГБ), от**
- **Объем жесткого диска (ГБ), до**
- **Объем оперативной памяти (МБ) от**
- **Объем оперативной памяти (МБ) до**

Информация о приложениях сторонних производителей

В разделе **Реестр приложений** можно настроить критерии включения устройств в выборку в зависимости от того, какие приложения на них установлены:

- **Название приложения**

  Раскрывающийся список, в котором можно выбрать приложение. Устройства, на которых установлено указанное приложение, будут включены в выборку.

- **Версия приложения**

  Поле ввода, в котором указывается версия выбранного приложения.

- **Производитель**

  Раскрывающийся список, в котором можно выбрать производителя установленного на устройстве приложения.

- **Статус приложения**

  Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении приложений, установленных на искомых устройствах. После установки флажка названия полей ввода **Название приложения**, **Версия приложения** и **Статус приложения** меняются на **Имя обновления**, **Версия обновления** и **Статус** соответственно.

  По умолчанию параметр выключен.

- **Название несовместимой приложения безопасности**

  Раскрывающийся список, в котором можно выбрать приложения безопасности сторонних производителей. Во время поиска устройства, на которых установлено выбранное приложение, будут включены в выборку.

- **Тег приложения**

  В раскрывающемся списке можно выбрать тег приложения. Все устройства, на которых установлены приложения, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

Если этот параметр выключен, критерий не применяется.

По умолчанию параметр выключен.

В разделе **Уязвимости и обновления** можно настроить критерии включения устройств в выборку по источнику обновлений Центра обновления Windows:

WUA переключен на Сервер администрирования

В раскрывающемся списке можно выбрать один из следующих вариантов поиска:

- **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 приложениях "Лаборатории Касперского"

В разделе **Приложения "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранного управляемого приложения:

- **Название приложения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию приложения "Лаборатории Касперского".

  В списке представлены названия только тех приложений, для которых на рабочем месте администратора установлены плагины управления.

  Если приложение не выбрано, то критерий не применяется.

- **Версия приложения**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии приложения "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 приложения наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Статус приложения**

  Раскрывающийся список, в котором можно выбрать статус приложения (*Установлено*, *Не установлено*). Устройства, на которых указанное приложение установлено или не установлено, 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 приложений, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей приложений, 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**. Приложение включает в выборку устройства, которые находятся под управлением Kaspersky Security Center.
- **Нет**. Приложение включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center.
- **Значение не выбрано**. Критерий не применяется.

- **Установлено приложение безопасности**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлено приложение безопасности:

  - **Есть**. Приложение включает в выборку устройства, на которых установлено приложение безопасности.
  - **Нет**. Приложение включает в выборку устройства, на которых не установлено приложение 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 приложения** содержит список компонентов тех приложений, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center Web Console.

В разделе **Компоненты приложения** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранному приложению:

- **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:

Применить, если есть хотя бы один из выбранных тегов

Если этот параметр включен, в результатах поиска отобразятся устройства, в описании которых есть хотя бы один из выбранных тегов.

Если этот параметр выключен, в результатах поиска отобразятся только устройства, в описаниях которых есть все выбранные теги.

По умолчанию параметр выключен.

Чтобы добавить теги к критерию, нажмите на кнопку **Добавить** и выберите теги, нажав на поле ввода **Тег**. Укажите, следует ли включать или исключать устройства с выбранными тегами в выборку устройств.

- **Должен присутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых есть выбранный тег. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

  По умолчанию выбран этот вариант.

- **Должен отсутствовать**

  Если выбран этот вариант, в результатах поиска отобразятся устройства, в описании которых нет выбранного тега. Для поиска устройств вы можете использовать символ *, который заменяет любую строку длиной 0 и более символов.

Пользователи

В разделе **Пользователи** можно настроить критерии включения устройств в выборку по учетным записям пользователей, выполнявших вход в операционную систему.

- **Последний пользователь, выполнивший вход в систему**
- **Пользователь, уже выполнявший вход в систему**

Если 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.

Владелец устройства

В разделе **Владелец устройства** вы можете настроить критерии включения устройств в выборку в соответствии с зарегистрированными владельцами устройства, их ролями и их членством в группах безопасности:

- **Владелец устройства**
- **Членство владельца устройства в группе безопасности Active Directory**
- **Роль владельца устройства**
- **Членство владельца устройства во внутренней группе безопасности**

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. 305).
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 приложения 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.

Теги устройств

В этом разделе описаны теги устройств, приведены инструкции по их созданию и изменению, а также по назначению тегов устройствам вручную и автоматически.

В этом разделе

См. также:

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. 304), при поиске устройств и при распределении устройств по группам администрирования (см. стр. 55).

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 приложениям 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 приложения 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 сетевых устройств 198

Изменение тегов устройств

► *Чтобы переименовать тег устройства:*

1. В главном окне приложения 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 сетевых устройств 198

Удаление тегов устройств

► *Чтобы удалить тег устройства:*

1. В главном окне приложения 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 приложением или Агентом администрирования. Для того чтобы удалить тег с вашего устройства, используйте утилиту klscflag.

См. также:

Сценарий: обнаружение сетевых устройств 198

Просмотр устройств, которым назначен тег

► *Чтобы просмотреть устройства с назначенными тегами:*

1. В главном окне приложения 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.

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 сетевых устройств 198

Просмотр тегов, назначенных устройству

► *Чтобы просмотреть теги, назначенные устройству:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В появившемся окне свойств устройства откройте вкладку **Теги**.

Отобразится список тегов, назначенных выбранному устройству.

Можно назначить другой тег (см. стр. 321) устройству или удалить назначенный ранее тег (см. стр. 322). Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

См. также:

Сценарий: обнаружение сетевых устройств 198

Назначение тегов устройству вручную

► *Чтобы вручную назначить тег устройству:*

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег (см. стр. 321).
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 сетевых устройств 198

kaspersky

Удаление назначенного тега с устройства

► *Чтобы снять назначенный тег с устройства:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В появившемся окне свойств устройства откройте вкладку **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. 320). Вы не можете вручную удалить теги, назначенные устройству приложениями или Агентом администрирования. Для того чтобы удалить эти теги, используйте утилиту klscflag.

См. также:

Сценарий: обнаружение сетевых устройств 198

Просмотр правил автоматического назначения тегов устройствам

► *Чтобы просмотреть правила автоматического назначения тегов устройствам,*

Выполните одно из следующих действий:

- В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне приложения 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. 321), и нажмите на кнопку **Свойства**.

Отобразится список правил автоматического назначения тегов устройствам.

См. также:

Сценарий: обнаружение сетевых устройств 198

Изменение правил автоматического назначения тегов устройствам

► *Чтобы изменить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 322).
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. 323).
   - Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры (см. стр. 323).
   - 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 сетевых устройств 198

Создание правил автоматического назначения тегов устройствам

► *Чтобы создать правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 322).
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.

- **Приложения** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Реестр приложений** – наличие на устройстве приложений 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. 323).
- После выполнения правила вручную (см. стр. 325).
- 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. 321) 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. 322).
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

См. также:

Сценарий: обнаружение сетевых устройств 198

Удаление правил автоматического назначения тегов с устройств

► *Чтобы удалить правило автоматического назначения тегов устройствам:*

1. Просмотрите правила автоматического назначения тегов устройствам (см. стр. 322).
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. 320).

См. также:

Сценарий: обнаружение сетевых устройств 198

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 приложений.

kaspersky

Вы можете использовать функцию шифрования данных, если в вашей сети есть управляемые устройства с операционной системой Windows, на которых установлено приложение 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/12.3/ru-RU/128080.htm, просматривать список зашифрованных жестких дисков (см. стр. 326), формировать и просматривать отчеты о шифровании (см. стр. 328).

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 справке Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/ru-RU/128080.htm.

Вы можете отобразить или скрыть некоторые элементы интерфейса, связанные с управлением шифрованием, с помощью параметров пользовательского интерфейса (см. стр. 195).

В этом разделе

См. также:

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 приложения 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. 195).

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.....393

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;
- приложению запрещен доступ к зашифрованному файлу;
- неизвестные ошибки.

► *Чтобы просмотреть список событий, возникших при шифровании данных на устройствах:*

В главном окне приложения 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. 195).

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 приложения 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.....393

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 приложений к зашифрованным файлам. Этот отчет полезен, если неавторизованный пользователь или приложение пытается получить доступ к зашифрованным файлам или жестким дискам.

Вы можете сгенерировать любой отчет в разделе **Мониторинг и отчеты** → **Отчеты** (см. стр. 561). 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. 195).
2. В главном окне приложения 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.....393

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 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 справке Kaspersky Endpoint Security для Windows, чтобы сгенерировать файл в Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/ru-RU/130941.htm.
2. В главном окне приложения 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 справке Kaspersky Endpoint Security для Windows (см. инструкции для Kaspersky Security Center Web Console в конце раздела) https://support.kaspersky.com/KESWin/12.3/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:

Совместимые приложения и решения "Лаборатории Касперского" 33

Сценарий: настройка защиты сети.....393

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. 454).

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера создания задачи **Новая задача** выберите приложение **Kaspersky Security Center 15** и тип задачи **Сменить Сервер администрирования**. Затем укажите устройства, для которых вы хотите сменить Сервер администрирования:

   - **Назначить задачу группе администрирования**

     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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

   - **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/12.3/ru-RU/128089.htm.

kaspersky

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 приложения 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 политик**

     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.

Отправка сообщения пользователям устройств

► *Чтобы отправить сообщение пользователям устройств:*

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

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Тип задачи** выберите **Отправка сообщений пользователю**.
4. Выберите параметр, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
5. Запустите созданную задачу.

После завершения работы задачи созданное сообщение будет отправлено пользователям выбранных устройств. Задача **Отправка сообщений пользователю** доступна только для устройств под управлением операционной системы Windows.

Удаленное включение, выключение и перезагрузка клиентских устройств

Kaspersky Security Center позволяет удаленно управлять клиентскими устройствами, включать, выключать и перезагружать их.

► *Чтобы удаленно управлять клиентскими устройствами:*

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

   Запустится мастер создания задачи.
3. В раскрывающемся списке **Тип задачи** выберите **Управление устройствами**.
4. Выберите параметр, чтобы указать группу администрирования, выборку устройств или устройства, к которым применяется задача.
5. Выберите команду (включить, выключить или перезагрузить). При желании можно указать сообщение пользователю и параметр **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)** для команд выключения и перезапуска.
6. Запустите созданную задачу.

После завершения работы задачи команда (включение, выключение или перезагрузка) будет выполнена на выбранных устройствах.

kaspersky

Развертывание приложений "Лаборатории Касперского"

В этом разделе описано, как развернуть приложения "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью Kaspersky Security Center Web Console.

В этом разделе

Сценарий: развертывание приложений "Лаборатории Касперского"

В этом сценарии описана процедура развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console. Можно либо воспользоваться мастером первоначальной настройки (см. стр. 143) и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Развертывание приложений "Лаборатории Касперского" состоит из следующих этапов:

1. Загрузка веб-плагина управления приложения

   Загрузите веб-плагин управления Kaspersky Endpoint Security для Linux https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint с сайта "Лаборатории Касперского" и добавьте плагин в Kaspersky Security Center Web Console.

z. **Создание инсталляционного пакета Агента администрирования**

   Создайте инсталляционный пакет Агента администрирования (см. стр. 338) из дистрибутива, входящего в комплект поставки.

   Вы можете использовать инсталляционный пакет для локальной установки Агента администрирования. Для этого следуйте инструкциям, приведенным в документации Kaspersky Endpoint Security для Linux https://support.kaspersky.com/help/KES4Linux/11.4.0/en-US/237152.htm.

aa. **Загрузка и создание инсталляционного пакета для Kaspersky Endpoint Security для Linux**

   Загрузите дистрибутив Kaspersky Endpoint Security для Linux https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint с сайта "Лаборатории Касперского" и создайте инсталляционный пакет Kaspersky Endpoint Security для Linux (см. стр. 338).

bb. **Создание автономного инсталляционного пакета (если требуется)**

   Если вы не можете установить приложения "Лаборатории Касперского" с помощью Kaspersky Security Center на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты (см. стр. 339) для приложений. Если вы используете автономные пакеты для установки программ "Лаборатории Касперского" пропустите пункты 5 и 6 этого сценария.

cc. **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. 454) 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 одного приложения 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. 358) и настройте Агент администрирования.

dd. **Создание и настройка задач**

   Задача *Установка обновлений* Kaspersky Endpoint Security для Linux должна быть настроена.

   Этот шаг входит в мастер первоначальной настройки: задача создается и настраивается автоматически, с параметрами по умолчанию. Если вы не запускали мастер первоначальной настройки, вам необходимо создать (см. стр. 454) и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи (см. стр. 456) соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

ee. **Создание политик**

Создайте политику Kaspersky Endpoint Security для Linux вручную (см. стр. 409) 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. 409) политики в соответствии с вашими требованиями.

ff. **Проверка результатов**

Убедитесь, что развертывание завершилось успешно: созданы политики и задачи для каждого приложения и эти приложения установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных приложений созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные приложения.

Добавление плагина управления для приложений "Лаборатории Касперского"

Чтобы развернуть приложение "Лаборатории Касперского", такую как Kaspersky Endpoint Security для Linux или Kaspersky Endpoint Security для Windows, необходимо загрузить веб-плагин управления для этого приложения.

► *Чтобы загрузить веб-плагин управления для приложения "Лаборатории Касперского":*

1. В главном окне приложения 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 приложения 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 в из файла и появится в списке веб-плагинов управления.

См. также:

Веб-плагин управления 56
Сценарий: развертывание приложений "Лаборатории Касперского" 333

Загрузка и создание инсталляционных пакетов для приложений "Лаборатории Касперского"

Если у Сервера администрирования есть доступ в интернет, вы можете создать инсталляционные пакеты приложений "Лаборатории Касперского" с веб-серверов "Лаборатории Касперского.

► *Чтобы загрузить и создать инсталляционный пакет для приложения "Лаборатории Касперского":*

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения перейдите в раздел **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Вы также можете просматривать информацию о новых пакетах для приложений "Лаборатории Касперского" в списке экранных уведомлений (см. стр. 600). 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. Выберите **Создать инсталляционный пакет для приложения "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 приложения 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 приложений "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 600

Сценарий: развертывание приложений "Лаборатории Касперского" 333

kaspersky

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любое приложение (такое как текстовый редактор) на клиентские устройства, например, с помощью задачи (см. стр. 452);
- создать автономный инсталляционный пакет (см. стр. 339).

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 приложения в тихом режиме.

► *Чтобы создать пользовательский инсталляционный пакет:*

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения 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. Выберите **Создать инсталляционный пакет из файла**.
4. Укажите имя инсталляционного 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 инсталляционный пакет из файла формата SFX (самораспаковывающийся архив) невозможно.

   Начнется загрузка файла на Сервер администрирования.
6. Если вы указали файл приложения "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение (см. стр. 368) для этого приложения. Чтобы продолжить, вам нужно 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. 370). Чтобы продолжить, вам нужно 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. 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 приложения 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. 139). 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 приложения.
  - **Приложение**. Название приложения, упакованного в пользовательский инсталляционные пакет.
  - **Версия**. Версия приложения.
  - **Язык**. Язык приложения, упакованного 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 600

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки приложений 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 приложения без участия Kaspersky Security Center. Вы можете создать автономный инсталляционный пакет для приложений "Лаборатории Касперского", так и для приложений сторонних производителей. Чтобы создать автономный инсталляционный пакет для приложений стороннего производителя, необходимо создать пользовательский инсталляционный пакет (см. стр. 338).

Убедитесь, что автономный инсталляционный пакет не доступен для третьих лиц.

► *Чтобы создать автономный инсталляционный пакет:*

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения 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. Убедитесь, что включен параметр **Установить Агент администрирования совместно с данным приложением**, если требуется установить Агент администрирования совместно с выбранным приложением.

   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 выбранного приложения уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вам нужно выбрать одно из следующих действий:
   - **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии приложения, и чтобы также остался автономный инсталляционный пакет для предыдущей версии приложения, 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 этого же приложения еще раз. Автономный инсталляционный пакет размещается в той же папке.
5. На шаге **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. 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. 139). Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных инсталляционных пакетов**, расположенную над списком инсталляционных пакетов.

См. также:

Сценарий: развертывание приложений "Лаборатории Касперского"..... 333

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. 93).
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 под учетной записью root:

   - Обычная локальная установка:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <число_байтов>
     ```

   - Установка на отказоустойчивый кластер Kaspersky Security Center:

     ```
     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. Подготовьте требуемое устройство с операционной системой Linux для удаленной установки (см. стр. 347). Загрузите и создайте пакет удаленной установки, используя пакет Агента администрирования .deb или .rpm, с помощью любой подходящей системы управления пакетами.
2. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat (см. стр. 358) и настройте Агент администрирования.
3. Прочитайте Лицензионное соглашение (см. стр. 368). Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.
4. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

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

5. Создайте файл ответов (в формате TXT) в каталоге, который вы указали в переменной среды. Добавьте в файл ответов список переменных в формате VARIABLE_NAME = variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вам нужно 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
6. Установка Агента администрирования:

   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     ```
     # rpm -i klnagent-<build number>.i386.rpm
     ```
   - Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
     ```
     # rpm -i klnagent64-<build number>.x86_64.rpm
     ```

- Чтобы установить Агент администрирования из RPM-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  `# rpm -i klnagent64-<build number>.aarch64.rpm`
- Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent_<build number>_i386.deb`
- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<build number>_amd64.deb`
- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<build number>_arm64.deb`

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

См. также:

Назначение пользователя владельцем устройства при установке Агента администрирования 497

Подготовка устройства под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования

Перед установкой Агента администрирования на устройство под управлением Astra Linux в режиме замкнутой программной среды вам нужно выполнить две подготовительные процедуры: одну, которая описана в приведенных ниже инструкциях, и общие подготовительные шаги для любого устройства с операционной системой Linux (см. стр. 347).

Предварительные условия:

- Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux (см. стр. 22).
- 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 подготовить устройство под управлением Astra Linux в режиме замкнутой программной среды к установке Агента администрирования:*

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 пакет совместимости:

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

3. Создайте директорию для ключа приложения:

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

4. Поместите ключ приложения 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.

5. Обновите оперативную память дисков:

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

   Перезагрузите систему.

6. Выполните шаги подготовки, общие для любого устройства с операционной системой Linux (см. стр. 347).

Устройство подготовлено. Теперь вы можете приступить к установке Агента администрирования (см. стр. 347).

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 приложения, включенного в пакет.
- **Название приложения**. Имя приложения, которое включено в автономный инсталляционный пакет.
- **Версия приложения**.

- **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 приложений "Лаборатории Касперского" и для приложений сторонних производителей, а также распространять инсталляционные пакеты на клиентские устройства и устанавливать приложения 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 приложений 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 приложения перейдите к вкладке **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 **Приложение** 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. 456). 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.

kaspersky

Подготовка устройства с операционной системой Linux и удаленная установка Агента администрирования на устройство с операционной системой Linux

Установка Агента администрирования состоит из двух шагов:

- Подготовка устройства с операционной системой Linux
- Удаленная установка Агента администрирования

Подготовка устройства с операционной системой Linux

► *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, приложение 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: `<имя пользователя> ALL = (ALL) NOPASSWD: ALL`. В этом случае `<имя пользователя>` 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 `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` в файл `/home/<имя пользователя>/.bashrc`, где `<имя пользователя>` — 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. 358) и настройте Агент администрирования.
5. Если вы хотите установить Агент администрирования на устройства с операционной системой Astra Linux, работающей в режиме замкнутой программной среды, выполните дополнительные действия для подготовки устройств Astra Linux (см. стр. 343).

Удаленная установка Агента администрирования

► *Чтобы установить Агент администрирования на устройство с операционной системой Linux:*

1. 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 Агента администрирования с помощью интерфейса приложения (см. стр. 336) или с веб-сайта "Лаборатории Касперского" https://www.kaspersky.ru/small-to-medium-business-security/downloads/endpoint.
   c. Для создания пакета удаленной установки используйте файлы:
      - klnagent.kpd;
      - akinstall.sh;
      - deb или rpm пакет Агента администрирования.
2. Создайте задачу удаленной установки приложения (см. стр. 349) 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.

3. Запустите задачу удаленной установки приложения. 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).

Установка приложений с помощью задачи удаленной установки

Kaspersky Security Center позволяет удаленно устанавливать приложения 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:

- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу 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.
- **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.

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. 359).

В этом разделе

Удаленная установка приложений

Этот раздел содержит информацию о том, как удаленно установить приложение на устройства в группе администрирования, устройства с определенными адресами или на выборку устройств.

► *Чтобы установить приложение на выбранные устройства:*

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

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка приложения**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

   - **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 приложения* 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 приложения, которое требуется установить.
   - В блоке параметров **Принудительная загрузка инсталляционного пакета** выберите способ доставки на клиентские устройства файлов, необходимых для установки приложения:

     - **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 параметр **С помощью Агента администрирования** включен, 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 приложение 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 приложения 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 приложения установки.

  Если количество попыток, указанное в параметрах задачи, превышено, Kaspersky Security Center больше не запускает приложение установки на устройстве. Чтобы перезапустить задачу *Удаленная установка приложения*, увеличьте значение параметра **Максимальное количество попыток установок** и запустите задачу. Также вы можете создать другую задачу *Удаленная установка приложения*.

- Если вы переносите данные из одного приложения "Лаборатории Касперского" в другое, и ваше текущее приложение защищено паролем, введите пароль в поле **Пароль для удаления приложения "Лаборатории Касперского"**. Обратите внимание, что во время переноса данных ваше текущее приложение "Лаборатории Касперского" будет удалено.

Поле **Пароль для удаления приложения "Лаборатории Касперского"** доступно, только если вы выбрали параметр **С помощью Агента администрирования** в группе параметров **Принудительно загрузить инсталляционный пакет**.

Вы можете использовать пароль удаления только для сценария переноса данных Kaspersky Security для Windows Server в Kaspersky Endpoint Security для Windows при установке Kaspersky Endpoint Security для Windows с помощью задачи *Удаленная установка приложения*. Использование пароля деинсталляции при установке других приложений может вызвать ошибки установки.

Для успешного завершения сценария переноса данных убедитесь, что выполнены следующие предварительные условия:

- Вы используете Агент администрирования Kaspersky Security Center версии 14.2 для Windows или выше.
- Вы устанавливаете приложение на устройства под управлением Windows.

- Настройте дополнительный параметр:
  - **Не устанавливать приложение, если оно уже установлено**

    Если этот параметр включен, выбранное приложение не устанавливается заново, если оно уже установлено на клиентском устройстве.

    Если этот параметр выключен, приложение будет установлено в любом случае.

    По умолчанию параметр включен.
  - **Предварительно проверять тип операционной системы перед загрузкой**
  - **Назначить установку инсталляционного пакета в групповых политиках Active Directory**

    Если этот параметр включен, инсталляционный пакет будет устанавливаться с помощью групповых политик Active Directory.

    Параметр доступен, если выбран инсталляционный пакет Агента администрирования.

    По умолчанию параметр выключен.
  - **Предлагать пользователю закрыть работающие приложения**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения 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 приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Выберите, на какие устройства вы хотите установить приложение:

- **Устанавливать на все устройства**

  Приложение 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**

  Приложение 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 приложений:

   - **Не перезагружать устройство**

     Если выбран этот вариант, устройство не будет перезагружаться после установки приложения безопасности.

   - **Перезагрузить устройство**

     Если выбран этот вариант, устройство будет перезагружено после установки приложения безопасности.

2. При необходимости на шаге **Выбор учетных записей для доступа к устройствам** добавьте учетные записи, которые будут использоваться для запуска задачи *Удаленная установка приложения*:

   - **Учетная запись не требуется (Агент администрирования уже установлен)**

     Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор приложения. 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 приложения.

Чтобы указать учетную запись пользователя, под которой будет запускаться приложение 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, выбранное приложение устанавливается на указанный набор устройств.

См. также:

Мастер развертывания защиты 150

Установка приложений на подчиненные Серверы администрирования

► *Чтобы установить приложение на подчиненные Серверы администрирования:*

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемому приложению 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. 454).
3. Создайте задачу удаленной установки приложения на подчиненных Серверах администрирования (см. стр. 349). Выберите тип задачи **Удаленная установка приложения на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранного приложения 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 выбранное приложение устанавливается на подчиненные Серверы администрирования.

kaspersky

Указание параметров удаленной установки на устройствах под управлением Unix

Когда вы устанавливаете приложение 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 приложения перейдите к вкладке **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 приложения** → **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 456

Сценарий: развертывание приложений "Лаборатории Касперского" 333

Сценарий: мониторинг и отчеты 544

Замещение приложений безопасности сторонних производителей

Для установки приложения безопасности "Лаборатории Касперского" средствами Kaspersky Security Center может потребоваться удалить приложение стороннего производителя, несовместимое с устанавливаемым приложением. Kaspersky Security Center предоставляет несколько способов удаления программ сторонних производителей.

Удаление несовместимых приложений при настройке удаленной установки приложения

Вы можете включить параметр **Удалять несовместимые приложения автоматически** во время настройки удаленной установки приложения безопасности в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые приложения перед установкой приложения безопасности на управляемое устройство (см. стр. 156).

Удаление несовместимых приложений с помощью отдельной задачи

Для удаления несовместимых приложений используется задача *Удаленная деинсталляция приложения* (см. стр. 454). Задачу следует запускать на устройствах перед задачей установки приложения безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача *Удаленная деинсталляция приложения*.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор приложения безопасности не может успешно удалить какое-либо из несовместимых приложений.

Удаленная деинсталляция приложений или обновлений программного обеспечения

Вы можете удаленно деинсталлировать приложения или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

► *Чтобы удаленно деинсталлировать приложения или обновления программного обеспечения:*

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

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center.
4. В списке **Тип задачи** выберите тип задачи **Удаленная деинсталляция приложения**.
5. В поле **Название задачи** укажите название новой задачи.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача (см. стр. 456).

   Перейдите к следующему шагу мастера.
7. Выберите, какое приложение вы хотите деинсталлировать, а затем выберите требуемые приложения, обновления или патчи, которые вы хотите удалить:
   - **Удалить управляемое приложение**
   - Удалить несовместимое приложение
   - **Удалить приложение из реестра приложений**
   - **Удалить указанное обновление приложения, патч или стороннее приложение**
8. 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**

Перейдите к следующему шагу мастера.

9. 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).

- **Спросить у пользователя**

  На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

  По умолчанию выбран этот вариант.

  - **Повторять запрос каждые (мин)**
  - **Принудительно перезагрузить через (мин)**

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения 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 приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

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 приложения. 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 на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, 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.

3. Нажмите на кнопку **Готово**.

   В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо.

   > Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

   Задача будет создана, настроена и отобразится в списке задач, в разделе **Активы (Устройства)** → **Задачи**.

4. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

   Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

   Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. стр. 456).

После завершения задачи, выбранное приложение будет удалено на выбранных устройствах.

См. также:

Замещение приложений безопасности сторонних производителей 355

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.

Если на устройстве нет ключей подписи GPG для SUSE Linux Enterprise, вы можете увидеть следующее предупреждение: `Package header is not signed!` Выберите параметр `i`, чтобы игнорировать предупреждение.

После подготовки устройства с операционной системой SUSE Linux Enterprise Server 15, установите Агент администрирования (см. стр. 333).

Подготовка устройства под управлением Windows к удаленной установке. Утилита riprep

Удаленная установка приложения 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 приложения 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 приложения 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.

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.

kaspersky

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).

Создание задачи Удаленное выполнение скриптов

Вы можете создать задачу *Удаленное выполнение скриптов* для выполнения инсталляционного пакета на клиентском устройстве и удаленной установки приложения.

Инсталляционный пакет содержит ZIP-архив с набором скриптов для выполнения на клиентских устройствах, а также файл manifest.json. Подробнее о создании этого типа инсталляционного пакета см. статью (см. стр. 364).

Эту задачу нужно запускать только на устройствах с Агентом администрирования для Linux.

► *Чтобы запустить задачу Удаленное выполнение скриптов:*

1. Перейдите в **Мастер создания задачи** и выберите тип задачи **Удаленное выполнение скриптов**.
2. Введите имя задачи и выберите устройства, которым будет назначена задача. Нажмите на кнопку **Далее**.
3. Выберите инсталляционный пакет на основе ZIP-архива с файлом manifest.json для удаленного выполнения.

   Если вы не хотите повторно запускать задачу на устройствах, на которых она уже была выполнена, включите параметр **Не запускать эту задачу на устройствах**, на которых она уже была выполнена.
4. Выберите учетную запись для запуска задачи.

   Если вы выберете учетную запись по умолчанию, то задачу будет выполнять Агент администрирования (учетная запись root).

   При запуске задачи *Удаленное выполнение скриптов* вы не можете изменить учетную запись, которая назначена задаче. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и создайте задачу снова с требуемой учетной записью.
5. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
6. Нажмите на кнопку **Готово**.

   Задача *Удаленное выполнение скриптов* создана и отображается в списке задач.

После получения данных из задачи *Удаленное выполнение скриптов*, Агент администрирования ограничивает доступ к полученным данным для всех пользователей, кроме администратора и пользователя, указанного в параметрах задачи.

kaspersky

В этом разделе

Создание инсталляционного пакета на основе манифест-файла

► *Чтобы создать инсталляционный пакета на основе манифест-файла:*

1. Выполните одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
   - В главном окне приложения 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. Выберите параметр **Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json**.
4. Укажите имя инсталляционного пакета и нажмите на кнопку **Обзор**.

   В открывшемся окне выберите файл для создания инсталляционного пакета.
5. Выберите архивный файл, расположенный на доступных дисках. О том, как подготовить архив для этой задачи, см. статью (см. стр. 365).

   Файл начнет загружаться на Сервер администрирования Kaspersky Security Center.

   Начнется процесс создания инсталляционного пакета.

   В окне мастера отобразится информация о завершении процесса.

   Если инсталляционный пакет не создан, отобразится соответствующее сообщение.
6. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования (см. стр. 139). После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя.** Название инсталляционного пакета.

- **Источник.** Имя поставщика приложения.
- **Версия.** Версия приложения.
- **Создан.** Дата создания инсталляционного пакета.
- **Изменен.** Дата изменения инсталляционного пакета.
- **Путь.** Путь к пользовательскому инсталляционному пакету на Сервере администрирования.

- Изменить имя пакета и параметры командной строки. Эта функция доступна только для пакетов, которые не созданы на основе приложений "Лаборатории Касперского".

Подготовка архива для задачи Удаленное выполнение скриптов

Архив для задачи *Удаленное выполнение скриптов* на основе файла manifest.json должен соответствовать следующим требованиям:

- Формат архива: ZIP.
- Общий размер: не более 1 ГБ.
- Количество файлов и папок в архиве не ограничено.
- Манифест-файл архива должен соответствовать приведенной ниже схеме и называться manifest.json. Схема проверяется только во время выполнения задачи на устройстве.

  Схема JSON манифест-файла и описание массивов

  Пример манифест-файла
- Архив должен иметь следующую структуру:

  manifest.json

  <файл1>

  <файл2>

  <папка1>/<файл3>

  <папка2>/<папка3>/<файл4>

  . . .

  <файлX>

  manifest.json – это манифест-файл задачи.

  <файл1>, ..., <файлX> – это набор файлов со скриптами, которые нужно выполнить.

Удаленная установка приложений на устройства с помощью задачи Удаленное выполнение скриптов

Задачу *Удаленное выполнение скриптов* можно использовать для удаленной установки приложения на клиентское устройство с помощью создания пользовательского инсталляционного пакета.

О том, как подготовить архив для этой задачи, см. статью (см. стр. 365).

Чтобы создать инсталляционный пакет для удаленной установки приложения на клиентское устройство, в архив, который вы хотите загрузить для этой задачи, должны быть включены следующие файлы:

- <package_name>.deb
- install.sh
- manifest.json

При запуске задачи *Удаленное выполнение скриптов* Агент администрирования загрузит инсталляционный пакет с приложением на клиентское устройство. Когда клиентское устройство получает инсталляционный пакет, Агент администрирования на этом устройстве анализирует файл manifest.json и определяет порядок выполнения скриптов и действий в зависимости от результата, а затем начинает выполнение.

После завершения задачи *Удаленное выполнение скриптов* приложение будет установлено на клиентском устройстве.

Настройка уведомлений и мониторинга для задачи Удаленное выполнение скриптов

Вы можете настроить мониторинг, поведение при сохранении событий и уведомления для задачи *Удаленное выполнение скриптов*.

► *Чтобы просмотреть статус задачи* Удаленное выполнение скриптов*:*

1. В главном окне приложения перейдите к вкладке **Устройства** → **Задачи**.

   Отобразится список задач.

2. Выберите задачу и нажмите на **История устройства**.

   Отображается ход выполнения задачи.

► *Чтобы настроить поведение при сохранении событий:*

1. В списке задач нажмите на имя задачи и перейдите на вкладку **Параметры**.
2. В разделе **Уведомления** нажмите на кнопку **Параметры**.
3. Выберите один из следующих вариантов поведения приложения после выполнения задачи:
   - **Сохранить все события**.
   - **Сохранять события о ходе выполнения задачи**.
   - **Сохранять только результат выполнения**.

     События сохраняются в разделе **История устройства** и **Хранилище событий**.

     По умолчанию сохраняются только результаты выполнения задачи.

     > Если вы выберете **Сохранить все события**, сохраняются только результаты выполнения задачи.

4. Если вы хотите сохранить события в базе данных Сервера администрирования, в журнале событий на Сервере администрирования или на устройстве, включите соответствующий параметр.

Подробнее о настройке уведомлений см. в этой статье.

kaspersky

Лицензирование

Этот раздел содержит информацию:

- Общие понятия, связанные с лицензированием Kaspersky Security Center.
- Инструкция по управлению лицензиями управляемых приложений "Лаборатории Касперского".

В этом разделе

См. также:

О лицензировании Kaspersky Security Center

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center.

В этом разделе

kaspersky

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

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 приложения. Если вы не согласны с условиями Лицензионного соглашения, вам нужно прервать установку приложения и не должны использовать приложение.

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 приложения зависят от лицензии, по которой используется приложение.

Предусмотрены следующие типы лицензий:

- *Пробная.*

  Бесплатная лицензия, предназначенная для ознакомления с приложением. Пробная лицензия имеет небольшой срок действия.

По истечении срока действия пробной лицензии Kaspersky Security Center прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

Вы можете использовать приложение по пробной лицензии только в течение одного пробного периода.

- *Коммерческая.*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии ключевые функции приложения 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 приложение 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 приложении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать приложение 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 приложение в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в приложение одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в приложение.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы приложения требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы приложения. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В приложении не может быть больше одного активного лицензионного ключа.

Дополнительный (резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование приложения, 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 автономном режиме:

- Вы можете ознакомиться с Политикой конфиденциальности перед установкой Kaspersky Security Center (см. стр. 93).
- 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 может работать в следующих режимах:

- **Базовая функциональность Консоли администрирования**

  Kaspersky Security Center работает в этом режиме до активации приложения или после истечения срока действия коммерческой лицензии. Приложение Kaspersky Security Center с поддержкой базовой функциональности Консоли администрирования поставляется в составе приложений "Лаборатории Касперского", предназначенных для защиты сети организации. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

- **Коммерческая лицензия**

  Если вам нужна дополнительная функциональность, не входящая в базовую функциональность Консоли администрирования, вам требуется приобрести коммерческую лицензию.

  При добавлении лицензионного ключа в окне свойств Сервера администрирования убедитесь, что вы добавили лицензионный ключ, который позволяет использовать Kaspersky Security Center. Вы можете найти эту информацию на сайте "Лаборатории Касперского". На странице каждого решения есть список приложений, включенных в это решение. Сервер администрирования может принимать неподдерживаемые лицензионные ключи, например лицензионный ключ для Kaspersky Endpoint

Security Cloud, но такие лицензионные ключи не предоставляют никаких новых функций, кроме базовой функциональности Консоли администрирования.

Функция или свойство	Режим работы Kaspersky Security Center	
	Лицензия отсутствует	Коммерческая лицензия
Базовая функциональность Консоли администрирования	✓	✓
Системное администрирование: базовая функциональность	✓	✓
Системное администрирование: расширенная функциональность	—	✓
Управление системами	—	✓
Экспорт событий в SIEM-системы с помощью формата Syslog	✓	✓
Экспорт событий в SIEM-системы: QRadar by IBM и ArcSight от Micro Focus	—	✓

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего приложение.

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 приложение 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.

kaspersky

О предоставлении данных

Данные, обрабатываемые локально

Приложение Kaspersky Security Center предназначено 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 приложений "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 приложений "Лаборатории Касперского" на устройства;
- управление параметрами работы и задачами установленных приложений;
- управление обновлениями приложений "Лаборатории Касперского" и других производителей, поиск и закрытие уязвимостей;
- активация приложений "Лаборатории Касперского" на устройствах;
- управление учетными записями пользователей;
- просмотр информации о работе приложений "Лаборатории Касперского" на устройствах;
- просмотр отчетов.

Для выполнения своих основных функций приложение 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 передает Агенту администрирования.
- 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 (для устройств, принадлежащих Windows-домену), имя устройства в среде (для устройств, принадлежащих Windows-домену), DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, серийный номер, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.
    - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств и для принятия решений о применимости тех или иных патчей и обновлений: 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 приложениях "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 приложениях "Лаборатории Касперского", установленных на устройстве. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования:
  - Параметры приложений "Лаборатории Касперского", установленных на управляемом устройстве: название и версия приложения "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 приложения, данные о параметрах и задачах приложения "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки приложения.
  - Статистика работы приложения: события, связанные с изменениями статуса компонентов приложения "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных компонентами приложения.
  - Состояние устройства, определенное приложением "Лаборатории Касперского".
  - Теги, передаваемые приложением "Лаборатории Касперского".
- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center и управляемых приложений "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.
- Данные, необходимые для интеграции Kaspersky Security Center с SIEM-системой для экспорта событий. Пользователь вводит данные в Консоли администрирования или Kaspersky Security Center Web Console.
- Настройки компонентов Kaspersky Security Center и управляемых приложений "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 приложений "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 приложениях и патчах, установленных на управляемых устройствах (Реестр приложений). Приложения могут быть сопоставлены с информацией об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений.

  - Данные об уязвимостях стороннего программного обеспечения, обнаруженных на управляемых устройствах.
  - Данные об обновлениях, доступных для сторонних приложений, установленных на управляемых устройствах.
- Данные, которые необходимы для загрузки обновлений на изолированный Сервер администрирования для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах. Пользователь вводит и передает данные с помощью утилиты klscflag Сервера администрирования.
- Пользовательские категории приложений. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль приложений. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Информация о шифровании устройств с операционной системой Windows и статусах шифрования. Управляемое приложение 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 приложений "Лаборатории Касперского". Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в резервное хранилище. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, помещенных в Карантин. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные о состоянии и срабатывании правил Адаптивного контроля аномалий. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- 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. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Информация о зашифрованных устройствах и статусе шифрования. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования.
- Информация об ошибках шифрования данных на устройствах. Шифрование выполняется функцией Шифрование данных приложений "Лаборатории Касперского". Управляемое приложение передает

данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.

- Список управляемых программируемых логических контроллеров (ПЛК). Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные для создания цепочки развития угроз. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Информация о попытках сотрудников организации получить доступ к облачным сервисам. Управляемое приложение передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующего приложения.
- Данные, необходимые для интеграции Kaspersky Security Center со службой Kaspersky Managed Detection and Response (для Kaspersky Security Center Web Console должен быть установлен специальный плагин): токен инициации интеграции, токен интеграции и токен сеанса пользователя. Пользователь с помощью токена инициации интеграции входит в интерфейс Kaspersky Security Center Web Console. Служба Kaspersky MDR передает токен интеграции и токен сеанса пользователя через специальный плагин.
- 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 номер телефона, пароль, секретный ключ, сгенерированный Сервером администрирования, и одноразовый пароль для двухэтапной проверки. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center Web Console.
- IP-адрес устройства, на котором пользователь создал ревизию. IP-адрес определяется Сервером администрирования автоматически.
- 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 приложений 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 соответствующего приложения.
- 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 и передает данные с помощью утилиты klsetsrvcert Сервера администрирования.
- Сертификаты для установки доверия к внутренним веб-ресурсам организации. 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 OpenAPI.
- 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 получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает данные от управляемого приложения "Лаборатории Касперского" и передает их на Сервер администрирования. Перечни данных, обрабатываемых управляемыми приложениями "Лаборатории Касперского", приведены в справках соответствующих приложений.
- Сервер администрирования самостоятельно получает данные 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 событий хранятся в незашифрованной 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 Kaspersky Security Center;
- версия Kaspersky Security Center;
- локализация Kaspersky Security Center;
- идентификатор лицензии;
- тип лицензии;

- признак покупки лицензии 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.

О подписке

Подписка на Kaspersky Security Center – это заказ на использование приложения с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложения сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность приложения сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании приложения по подписке Kaspersky Security Center автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Если доступ к серверу через системный DNS невозможен, приложение использует публичные DNS-серверы (см. стр. 194). Вы можете продлить подписку на веб-сайте поставщика услуг.

Активация Kaspersky Security Center

Вы можете активировать Kaspersky Security Center, чтобы использовать его дополнительные функции. Эту задачу можно выполнить двумя способами: с помощью мастера первоначальной настройки Сервера администрирования или с помощью настройки параметров Сервера администрирования (см. стр. 148).

► *Чтобы активировать Kaspersky Security Center:*

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 **Лицензионные ключи**.
3. В разделе **Действующая лицензия** нажмите на кнопку **Выбрать**.
4. В открывшемся окне выберите лицензионный ключ, который вы хотите использовать для активации Kaspersky Security Center. Если лицензионного ключа нет в списке, нажмите на кнопку **Добавить лицензионный ключ** и укажите новый лицензионный ключ.
5. При необходимости вы также можете добавить резервный лицензионный ключ. Для этого в разделе **Резервный лицензионный ключ** нажмите на кнопку **Выбрать** и выберите существующий лицензионный ключ или добавьте ключ. Обратите внимание, что вы не можете добавить резервный лицензионный ключ, если нет активного лицензионного ключа.
6. Нажмите на кнопку **Сохранить**.

См. также:

Лицензирование управляемых приложений "Лаборатории Касперского"

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых приложений "Лаборатории Касперского".

Kaspersky Security Center позволяет централизованно распространять лицензионные ключи приложений "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 приложение 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.

kaspersky

В этом разделе

См. также:

Лицензирование управляемых приложений

Приложения "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждому из приложений. Файл ключа или код активации может быть распространен следующими способами:

- с помощью автоматического распространения;
- с помощью инсталляционного пакета управляемого приложения;
- с помощью задачи добавления лицензионного ключа управляемого приложения;
- активация управляемого приложения вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Приложение "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Приложение, 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 приложения 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 установлено приложение безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Linux. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Приложение 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 невозможно 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. 386), 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. 381)
- Автоматическое распространение лицензионного ключа (см. стр. 384)

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Добавление файла ключа или кода активации в инсталляционный пакет управляемого приложения

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемого приложения с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этого приложения. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Добавление лицензионного ключа в инсталляционный пакет (см. стр. 152).

Распространение с помощью задачи добавления лицензионного ключа управляемого приложения

В случае использования задачи добавления лицензионного ключа управляемого приложения 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. 381)
- Распространение лицензионного ключа на клиентские устройства (на стр. 382)

Добавление кода активации или файла ключа вручную на устройства

Вы можете активировать установленное приложение "Лаборатории Касперского" локально, используя инструменты приложения. Дополнительную информацию см. в документации к установленным приложениям.

Добавление лицензионного ключа в хранилище Сервера администрирования

► *Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:*

1. В главном окне приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на кнопку **Добавить**.
3. Выберите то, что вы хотите добавить:
   - **Добавить файл ключа.**

     Нажмите на кнопку **Выберите файл ключа** и выберите файл .key, который вы хотите добавить.
   - **Ввести код активации.**

     Укажите код активации в текстовом поле и нажмите на кнопку **Отправить**.
4. Нажмите на кнопку **Закрыть**.

Лицензионный ключ или несколько лицензионных ключей добавлены в хранилище Сервера администрирования.

См. также:

kaspersky

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center Web Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи добавления лицензионного ключа.

Добавление лицензионного ключа в хранилище Сервера администрирования (на стр. 381).

► *Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи добавления ключа:*

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

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите приложение, для которого вы хотите добавить лицензионный ключ.
4. В списке **Тип задачи** выберите задачу **Добавить ключ**.
5. В поле **Название задачи** укажите название новой задачи.
6. Выберите устройства, которым будет назначена задача (см. стр. 456).
7. На шаге мастера **Выбор лицензионного ключа** перейдите по ссылке **Добавить ключ**, чтобы добавить лицензионный ключ.
8. В панели добавления ключа добавьте лицензионный ключ, используя один из следующих параметров:

   Вам необходимо добавить лицензионный ключ только в том случае, если вы не добавляли его в хранилище Сервера администрирования до создания задачи добавления ключа.

   - Выберите параметр **Ввести код активации**, чтобы ввести код активации, а затем выполните следующие действия:

     a. Укажите код активации и нажмите на кнопку **Отправить**.

        Информация о лицензионном ключе отображается в панели добавления ключа.

     b. Нажмите на кнопку **Сохранить**.

        Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

        Панель добавления ключа закрыта.
   - Выберите параметр **Добавить файл ключа**, чтобы добавить файл ключа, и выполните следующие действия:

     a. Нажмите на кнопку **Выберите файл ключа**.

     b. В открывшемся окне выберите файл ключа и нажмите на кнопку **Открыть**.

Информация о лицензионном ключе отображается в панели добавления лицензионного ключа.

c. Нажмите на кнопку **Сохранить**.

> Если вы хотите автоматически распространять лицензионный ключ на управляемые устройства, включите параметр **Автоматически распространять лицензионный ключ на управляемые устройства**.

Панель добавления ключа закрыта.

9. Выберите лицензионный ключ в таблице ключей.
10. На шаге мастера **Информация о лицензии** включите параметр **Использовать как резервный ключ**, если вы хотите использовать этот ключ в качестве резервного.

    В этом случае резервный ключ применяется после истечения срока действия активного ключа.
11. Если на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, 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.
12. Нажмите на кнопку **Готово**.

    В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо (см. стр. 456).

    > Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

    Задача будет создана, настроена и отобразится в списке задач.
13. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

    Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

    Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. стр. 456).

После завершения задачи, лицензионный ключ распространится на выбранные устройства.

См. также:

Автоматическое распространение лицензионного ключа

Kaspersky Security Center позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

► *Чтобы автоматически распространять лицензионный ключ на управляемые устройства:*

1. В главном окне приложения 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 приложения 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.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для приложения.
- Виртуальный Сервер администрирования не имеет управляемых устройств.
- Лицензионный ключ уже используется для устройств, управляемых другим виртуальным Сервером администрирования, и достигнуто лицензионное ограничение на количество устройств.

Виртуальный Сервер администрирования автоматически распространяет лицензионные ключи из своего хранилища и из хранилища Сервера администрирования. Рекомендуется:

- Используйте задачу *Добавить лицензионный ключ*, чтобы выбрать лицензионный ключ, который необходимо развернуть на устройствах.
- Не выключайте параметр **Разрешить автоматическое распространение лицензионных ключей этого виртуального Сервера на его устройства** в параметрах виртуального Сервера администрирования. Иначе виртуальный Сервер администрирования не будет распространять лицензионные ключи на устройства, в том числе лицензионные ключи из хранилища Сервера администрирования.

Если вы установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**, соответствующий лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете позже вручную распространить лицензионный ключ.

См. также:

Просмотр информации об используемых лицензионных ключах

► *Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:*

В главном окне приложения 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 приложения 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 вкладке **Общие** – основную информацию о лицензионном ключе.
- На вкладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленного приложения "Лаборатории Касперского".

► *Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства перейдите на вкладку **Приложения**.
4. Нажмите на название приложения, для которого вы хотите просмотреть информацию о распространенном лицензионном ключе.
5. В открывшемся окне свойств приложения перейдите на вкладку **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, приложение использует публичные DNS-серверы (см. стр. 194).

См. также:

События превышения лицензионного ограничения

Kaspersky Security Center позволяет получать информацию о событиях превышения лицензионного ограничения приложений "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, приложения 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 приложения 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. 381) 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 управляемого приложения "Лаборатории Касперского". Вам нужно удалить выбранное приложение, прежде чем отзывать его Лицензионное соглашение.

► *Чтобы отозвать Лицензионное соглашение для управляемых приложений "Лаборатории Касперского":*

1. Откройте окно свойств Сервера администрирования и на вкладке **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 приложение "Лаборатории Касперского", которому 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; приложение больше не установлено.

Продление срока действия лицензии приложений "Лаборатории Касперского"

Вы можете продлить срок действия лицензии приложений "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 приложения перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
- В главном окне приложения 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

Использование Kaspersky Marketplace для выбора бизнес-решений

Marketplace – раздел главного меню, позволяющий просмотреть весь спектр бизнес-решений "Лаборатории Касперского", выбрать те, которые вам нужны, и перейти к покупке на сайте "Лаборатории Касперского". Вы можете использовать фильтры для просмотра только тех решений, которые соответствуют вашей организации и требованиям вашей системы информационной безопасности. Когда вы выбираете решение, Kaspersky Security Center перенаправляет вас на соответствующую страницу на сайте "Лаборатории Касперского", чтобы вы могли узнать о решении подробнее. Каждая веб-страница позволяет вам перейти к покупке или содержит инструкции по процессу покупки.

В разделе **Marketplace** вы можете фильтровать решения "Лаборатории Касперского" по следующим критериям:

- Количество устройств (конечных точек, серверов и других типов активов), которые вы хотите защитить:
  - 50–250
  - 250–1000
  - Более 1000
- Уровень опытности команды информационной безопасности вашей организации:
  - **Foundations**

    Этот уровень типичен для предприятий, в которых есть только ИТ-команда. Максимально возможное количество угроз блокируется автоматически.
  - **Optimum**

    Этот уровень типичен для предприятий, у которых есть конкретная функция ИТ-безопасности в ИТ-команде. На этом уровне компаниям требуются решения, которые позволят им противостоять товарным угрозам и угрозам в обход существующих превентивных механизмов.
  - **Expert**

    Этот уровень типичен для предприятий со сложной и распределенной ИТ-средой. Группа ИТ-безопасности состоит из опытных специалистов, или в компании есть группа SOC (Security Operations Center). Необходимые решения позволяют компаниям противостоять комплексным угрозам и целевым атакам.
- Типы активов, которые вы хотите защитить:
  - **Конечные точки**: рабочие станции сотрудников, физические и виртуальные машины, встраиваемые системы.
  - **Серверы**: физические и виртуальные серверы.
  - **Cloud**: публичные, частные или гибридные облачные среды; облачные сервисы.
  - **Сеть**: локальная сеть, ИТ-инфраструктура.
  - **Услуга**: услуги, связанные с безопасностью, предоставляемые "Лабораторией Касперского".

► *Чтобы найти и приобрести бизнес-решение "Лабораторией Касперского":*

1. В главном окне приложения перейдите в раздел **Marketplace**.

   По умолчанию в разделе отображаются все доступные бизнес-решения "Лаборатории Касперского".

2. Чтобы просмотреть только те решения, которые подходят вашей организации, выберите нужные значения в фильтрах.
3. Нажмите на решение, которое вы хотите приобрести или о котором хотите узнать больше.

Вы будете перенаправлены на веб-страницу решения. Следуйте инструкциям на экране, чтобы перейти к покупке.

См. также:

kaspersky

Настройка приложений "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:

kaspersky

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. 93).
- Установили Kaspersky Security Center Web Console (см. стр. 104).
- Основной сценарий установки Kaspersky Security Center завершен.
- Мастер первоначальной настройки (см. стр. 143) завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования;
  - задача *Поиск уязвимостей и требуемых обновлений.*

Этапы

Настройка защиты сети состоит из следующих этапов:

1. Настройка и распространение политик и профилей политик для приложений "Лаборатории Касперского"

   Для настройки и распространения параметров приложений "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью (см. стр. 394): ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

gg. Настройка задач для удаленного управления приложениями "Лаборатории Касперского"

Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

Инструкции: Настройка групповой задачи обновления Kaspersky Endpoint Security(см. стр. 444), Создание задачи Поиск уязвимостей и требуемых обновлений (см. стр. 682).

При необходимости создайте дополнительные задачи управления приложениями "Лаборатории Касперского", установленными на клиентских устройствах.

hh. Оценка и ограничение загрузки событий в базу данных

Информация о событиях в работе управляемых приложений 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. 188).

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке приложений "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Приложения "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление приложениями 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 приложений "Лаборатории Касперского" (см. стр. 515).

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....515

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 приложений к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства (см. стр. 395), позволяет вам применять различные параметры приложения 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. 397), позволяет вам применять различные параметры приложений безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры приложения для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры приложений 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 приложениями "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры приложения могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры приложений 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 приложения. 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. 404) 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. 513).

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center (см. стр. 93) и Kaspersky Security Center Web Console (см. стр. 104). Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователя (см. стр. 397) как альтернативу или дополнительную возможность для подхода, ориентированного на устройства. Узнайте больше о двух подходах к управлению (см. стр. 394).

Этапы

Сценарий управления приложениями «Лаборатории Касперского», ориентированный на устройства, содержит следующие шаги:

1. Настройка политик приложений

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики (см. стр. 409) для каждого приложения. 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 приложений:

   - 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 этого приложения.

   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. 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. 409).

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. 404) 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. 318). 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 приложения "Лаборатории Касперского" будут управляться своим профилем политики.

   Инструкции:

   - Создание профиля политики (см. стр. 420)
   - Создание правила активации профиля политики (см. стр. 421)

3. **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 приложениям "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. 415).

Результаты

После завершения сценария, ориентированного на устройства, приложения "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики приложений и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

kaspersky

См. также:

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке приложений "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария приложения будут настроены на всех управляемых устройствах в соответствии с политиками приложений и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center (см. стр. 93) и Kaspersky Security Center Web Console (см. стр. 104) и завершили основной сценарий установки. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства (см. стр. 395) как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению (см. стр. 394).

Процесс

Сценарий управления приложениями "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. Настройка политик приложений

   Настройте параметры установленных приложений "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждого приложения. 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 этого приложения.

   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. 401). Остальные незаблокированные

параметры будут доступны для изменения в политике ниже по иерархии. Созданная иерархия политик (см. стр. 403) позволяет эффективно управлять устройствами в группах администрирования.

Инструкция: Создание политики (см. стр. 409).

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующие роли.

   Инструкция: Назначение пользователя владельцем устройства (см. стр. 496).

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вам нужно 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 приложения, 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 приложения.

   Инструкция: Создание роли пользователя (см. стр. 511).

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. 512).

6. **Создание профилей политики**

   Создайте профиль политики (см. стр. 404) для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к приложениям, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики (см. стр. 420)

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 приложениям "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкция: Связь профилей политики с ролями (см. стр. 513).

8. **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 приложениям "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. 415).

Результаты

После завершения сценария, ориентированного на пользователя, приложения "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 приложений и профили политик будут автоматически применяться к устройствам этого пользователя.

См. также:

kaspersky

Политики и профили политик

В Kaspersky Security Center Web Console можно создавать политики для приложений "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 393

О политиках и профилях политик

Политика – это набор параметров приложения "Лаборатории Касперского", которые применяются к группе администрирования (см. стр. 55) и ее подгруппам. Вы можете установить несколько приложений "Лаборатории Касперского" (см. стр. 33) на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждого приложения "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Таблица 37. Статус политики

Состояние	Описание
Активная	Это текущая политика, которая применяется к устройству. Для приложения "Лаборатории Касперского" в каждой группе администрирования может быть активна только одна политика. Значения параметров активной политики приложения "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 одного приложения можно настроить несколько политик с различными значениями.

- Для одного приложения 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 локального приложения, 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 402

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка ( ). В таблице ниже показаны состояния значка замка:

Таблица 38. Статусы значка замка

Состояние	Описание
Не определено	Если рядом с параметром отображается значок открытого замка и переключатель выключен, параметр не указан в политике. Пользователь может изменить эти параметры в интерфейсе управляемого приложения. Такие параметры называются *разблокированными*.
Принудительно	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 управляемого приложения. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами приложения "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

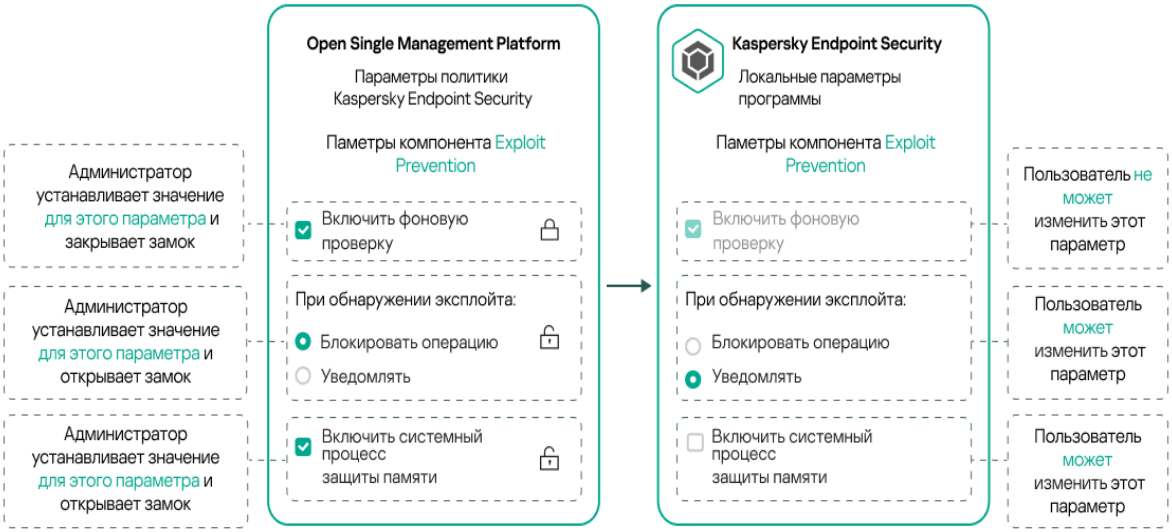
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров приложения "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров приложения "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемое приложение "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры приложения "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.....404

Иерархия политик.....403

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

kaspersky

В этом разделе

Иерархия политик

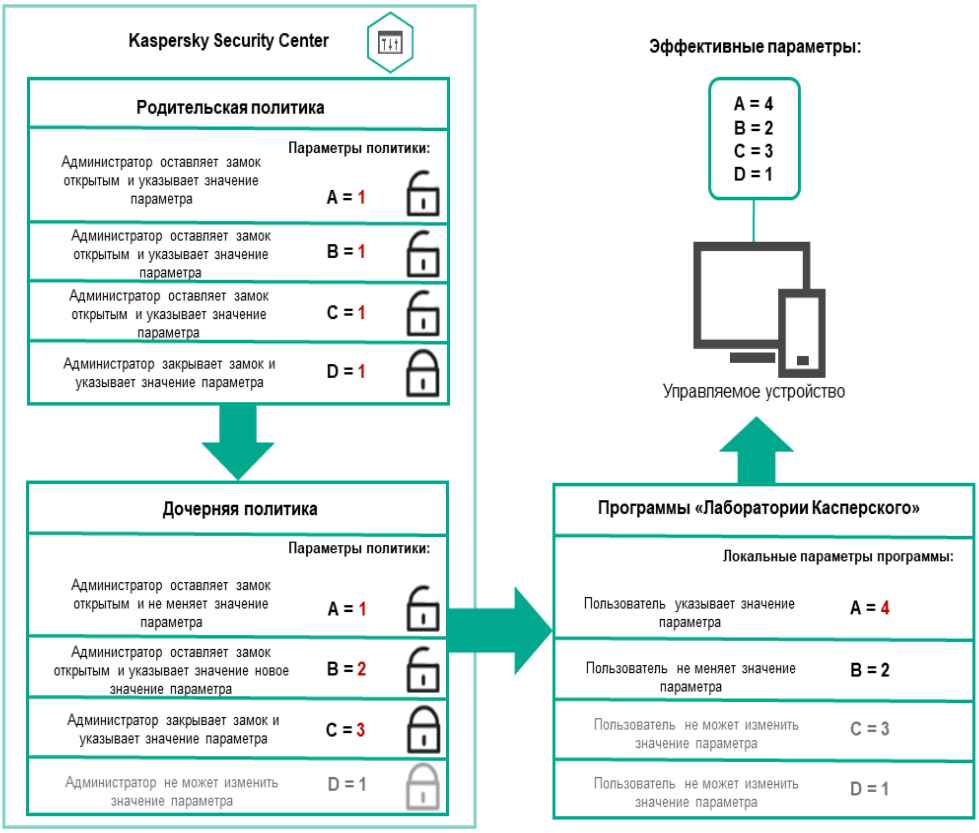
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования (см. стр. 55). 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.

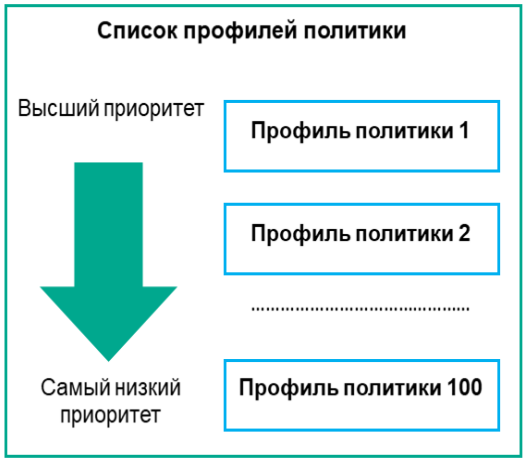
Политики одного и того же приложения действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).



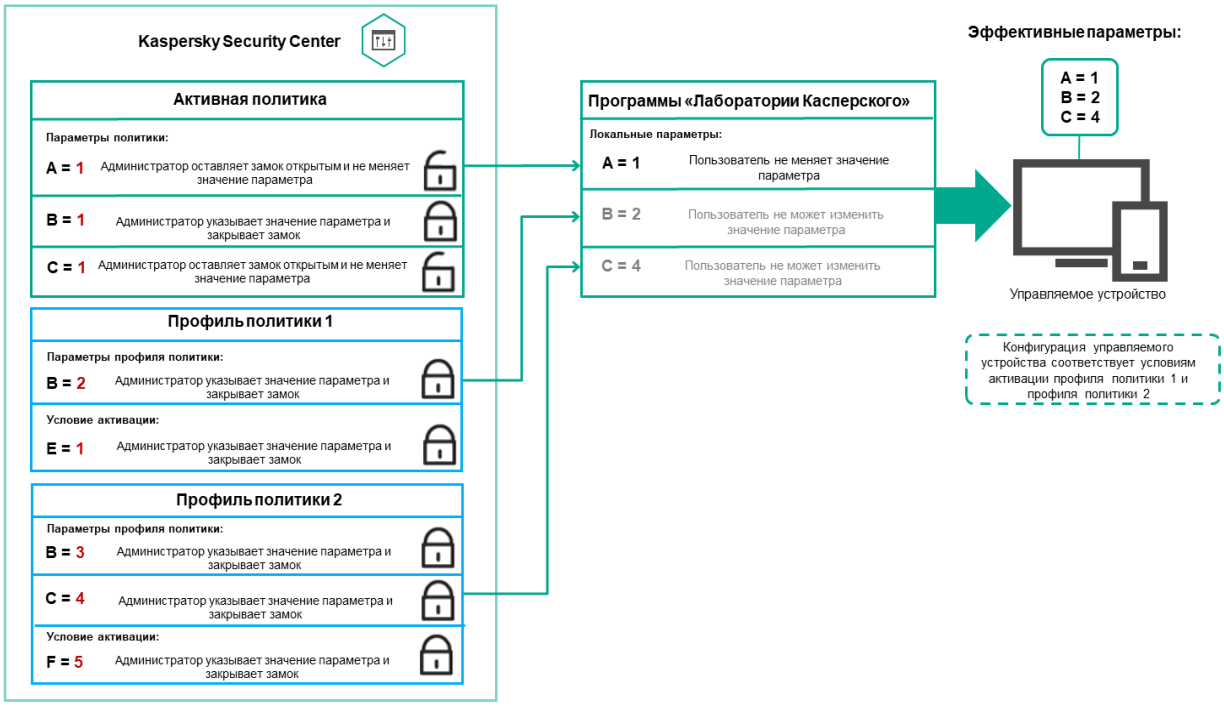
Профили политик в иерархии политик

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).



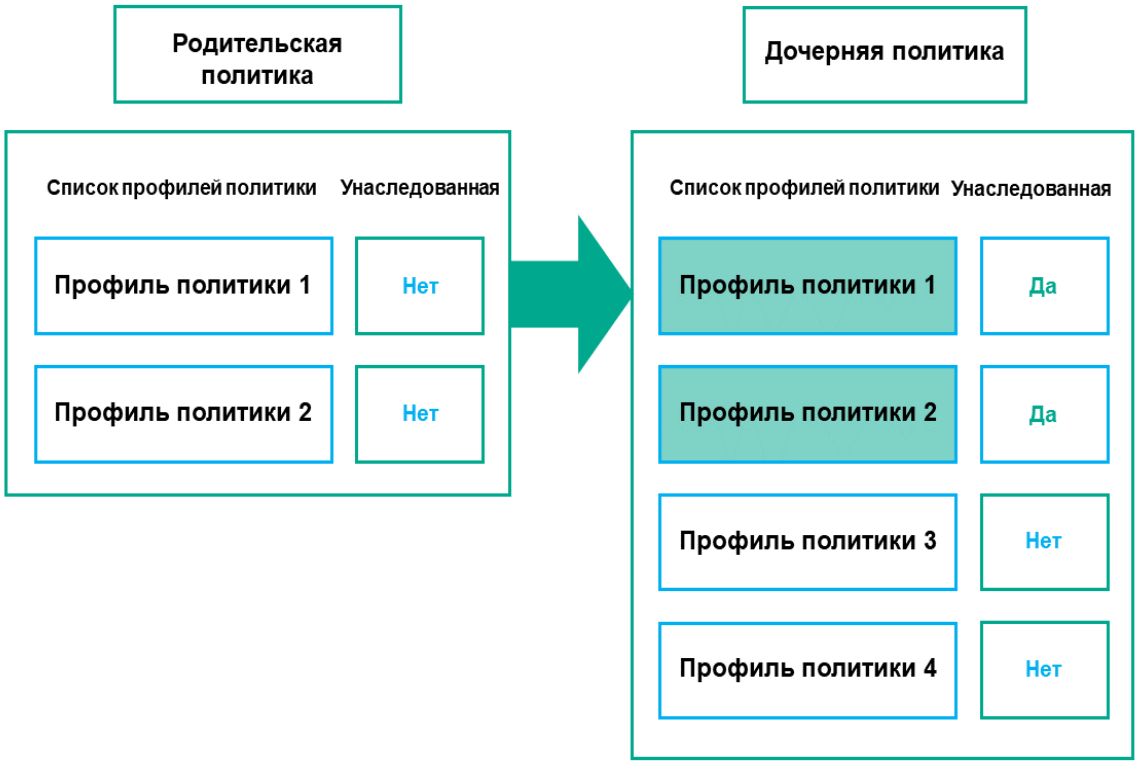
- Условия активации профилей политик не зависят друг от друга. Одновременно можно активировать несколько профилей политик. Если несколько профилей политики влияют на один и тот же параметр, устройство использует значение параметра из профиля политики с наивысшим приоритетом (см. рисунок ниже).



Профили политик в иерархии наследования

Профили политик из политик разных уровней иерархии соответствуют следующим условиям:

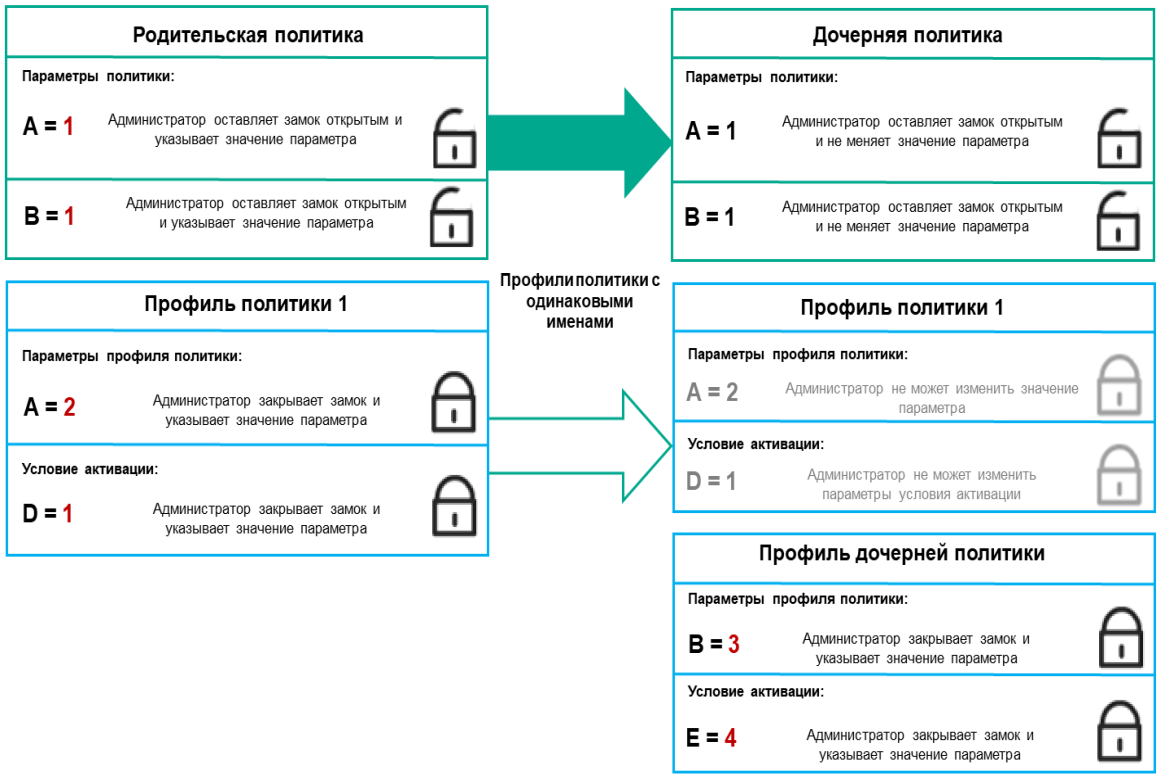
- Политика нижнего уровня наследует профили политики из политики более высокого уровня. Профиль политики, унаследованный от политики более высокого уровня, получает более высокий приоритет, чем уровень исходного профиля политики.
- Вы не можете изменить приоритет унаследованного профиля политики (см. 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 395

Как параметры реализованы на управляемом устройстве

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемого приложения.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

См. также:

kaspersky

Управление политиками

В этом разделе описывается управление политиками и предоставляется 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 приложения 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:

Сценарий: настройка защиты сети ... 393

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

► *Чтобы создать политику:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Выбрать приложение**.
3. Выберите приложение, для которого требуется создать политику.
4. Нажмите **Далее**.

   Откроется окно параметров новой политики на вкладке **Общие**.
5. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.
6. Перейдите на вкладку **Параметры приложения**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.
7. В левой области вкладки **Параметры приложения** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования (см. стр. 173)
   - Параметры политики Агента администрирования (см. стр. 425)
   - Справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/index.htm
   - Справка Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/ru-RU/222859.htm

   Подробнее о параметрах других приложений безопасности см. в документации к соответствующему приложению.

   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 приложений "Лаборатории Касперского"..... 333

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 вкладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на вкладках:

- **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**

- **Уведомления о событиях**

  Вы можете выбрать способ уведомления о событии:

  - **Уведомлять по электронной почте**
  - **Уведомлять по SMS**
  - **Уведомлять запуском исполняемого файла или скрипта**
  - **Уведомлять по SNMP**

  По умолчанию используются параметры уведомлений, указанные на вкладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на вкладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

История ревизий

На вкладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат (см. стр. 636).

См. также:

Сценарий: настройка защиты сети.....393

Изменение политики

► *Чтобы изменить политику:*

1. В главном окне приложения 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. 410) и параметры приложения, для которого вы создаете политику. Подробную информацию см. в следующих источниках:
   - Настройка Сервера администрирования (см. стр. 173)
   - Параметры политики Агента администрирования (см. стр. 425)
   - Справка Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/index.htm

- Справка Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/ru-RU/222859.htm

Подробнее о параметрах других приложений безопасности см. в документации к этим приложениям.

4. Нажмите на кнопку **Сохранить**.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

Включение и отключение параметра наследования политики

► *Чтобы включить или выключить параметр наследования в политике:*

1. Откройте требуемую политику.
2. Откройте вкладку **Общие**.
3. Включение или выключение 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 403

Сценарий: настройка защиты сети 393

Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

► *Чтобы скопировать политику в другую группу администрирования:*

1. В главном окне приложения 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.....393

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 приложения 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.....393

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. 414).

► *Чтобы экспортировать политику:*

1. В главном окне приложения 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. 414).

► *Чтобы импортировать политику:*

1. В главном окне приложения 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 приложения 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**.

Приложение 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. 304), 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**.

   Приложение 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 приложения "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 приложения на управляемые устройства:*

1. В главном окне приложения 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 вкладку **Приложения**.
4. Выберите приложение, для которого требуется посмотреть дату синхронизации политики.

   Откроется окно политики приложения, 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 приложения 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 100 000.

► *Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:*

1. В главном меню перейдите в параметры своей учетной записи и выберите **Параметры интерфейса**.

2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.

3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Автоматическая активация политики по событию "Вирусная атака"

► *Чтобы политика активировалась автоматически при наступлении события "Вирусная атака":*

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования на вкладке **Общие**.

2. Выберите раздел **Вирусная атака**.
3. В правой панели нажмите на ссылку **Настроить активацию политик по возникновению события "Вирусная атака"**.

   Откроется окно **Активация политик**.

4. В разделе, к которому относится компонент обнаруживший вирусную атаку (антивирусы для рабочих станций и файловых серверов, антивирусы для почтовых серверов, антивирусы защиты периметра), выберите нужную вам записью и затем нажмите на кнопку **Добавить**.

   Откроется окно с группой администрирования **Управляемые устройства**.

5. Нажмите на значок шеврона () рядом с **Управляемые устройства**.

   Отобразится иерархия групп администрирования и их политик.

6. В иерархии групп администрирования и их политик нажмите на имя политики (или политик), которая активируется при возникновении вирусной атаки.

   Чтобы выбрать все политики в списке или в группе, установите флажок рядом с требуемым именем.

7. Нажмите на кнопку **Сохранить**.

   Окно с иерархией групп администрирования и их политиками закрыто.

Выбранные политики добавляются в список политик, которые активируются при возникновении вирусной атаки. Выбранные политики активируются во время вирусной атаки независимо от того, активны они или неактивны.

В случае активации политики по событию Вирусная атака вернуться к предыдущей политике можно только вручную.

См. также:

Сценарий: мониторинг и отчеты 544
Сценарий: настройка защиты сети 393

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 приложения 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 393

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 приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на вкладке **Общие**.
3. Откройте вкладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

См. также:

Сценарий: настройка защиты сети 393

Изменение приоритета профиля политики

► *Чтобы изменить приоритет профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 419).

   Откроется список профилей политики.
2. На вкладке **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 404
Наследование политик и профилей политик 402
Сценарий: настройка защиты сети 393

Создание профиля политики

► *Чтобы создать профиль политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 419).

   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 вкладку **Параметры приложения**.

   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 вкладки **Параметры приложения** 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 395
Сценарий: настройка защиты сети 393

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. 419).

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На вкладке **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.....393

Создание правила активации профиля политики

► *Чтобы создать правило активации профиля политики:*

1. Перейдите к списку профилей выбранной политики (см. стр. 419).

   Откроется список профилей политики.

2. На вкладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики (см. стр. 420).

3. На вкладке **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 профиля политики 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.

- **Применить 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 вкладке **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. 419).

   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 приложений, установленных на устройствах групп нижнего уровня.

См. также:

Сценарий: настройка защиты сети 393

kaspersky

Параметры политики Агента администрирования

► *Чтобы настроить параметры политики Агента администрирования:*

1. В главном окне приложения 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. 435).

Общие

На этой закладке можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активная 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. 61) меньше 2 ГБ (для установки приложений 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. 273).

Параметры приложения

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. 518).

Обратите внимание, что приложения безопасности на управляемых устройствах получают обновления от источника, заданного в задаче обновления для каждого приложения 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.

- **Приложение может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в приложение безопасности (например, Kaspersky Endpoint Security для Linux). Передаваемая информация отображается в интерфейсе приложения 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 приложениях**

  Если этот параметр включен, на Сервер администрирования отправляется информация о приложениях, 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-порт** укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

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 приложения, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для приложения политика для автономных пользователей не определена, приложение будет использовать активную политику.

  Если параметр выключен, приложения 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 приложение 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-порт**

укажите номер порта. По умолчанию параметр включен. По умолчанию подключение к прокси-серверу KSN выполняется через UDP-порт 15111.

Обновления (точки распространения)

В разделе **Обновления (точки распространения)** вы можете включить функцию загрузки файлов различий, так как точки распространения получают обновления в виде файлов различий с серверов обновлений "Лаборатории Касперского" (см. стр. 539).

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....515

Сравнение параметров Агента администрирования по операционным системам 435

Использование Агента администрирования для Windows, Linux и macOS: сравнение

Использование Агента администрирования зависит от операционной системы устройства. Свойства политики Агента администрирования и инсталляционного пакета зависят от операционной системы (см. стр. 267). В таблице ниже сравниваются возможности и сценарии использования Агента администрирования, доступные для операционных систем Windows, Linux и macOS.

Таблица 39. Сравнение функций Агента администрирования

Функция Агента администрирования	Windows	Linux	macOS
Установка			
Установка методом клонирования образа жесткого диска администратора с операционной системой и Агентом администрирования сторонними средствами (см. стр. 243).	✓	✓	✓
Установка приложений с помощью сторонних средств удаленной установки приложений	✓	✓	✓
Установка вручную с помощью запуска инсталляторов приложений на устройствах	✓	✓	✓
Установка Агента администрирования в тихом режиме (см. стр. 250).	✓	✓	✓
Подключение клиентского устройства к Серверу администрирования вручную	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Автоматическая установка обновлений и патчей для компонентов Kaspersky Security Center	✓	—	—
Автоматическое распространение ключа	✓	✓	✓
Принудительная синхронизация	✓	✓	✓
Точка распространения			
Использование точки распространения (см. стр. 233).	✓	✓	✓
Автоматическое назначение точек распределения (см. стр. 234).	✓	✓ Без использования Network Location Awareness (NLA).	✓ Без использования Network Location Awareness (NLA).
Офлайн-модель получения обновлений	✓	✓	✓
Опрос сети	✓ • Опрос IP-диапазонов • Опрос контроллеров домена	✓ • Опрос IP-диапазонов • Опрос Zeroconf • Опрос контроллеров домена (Microsoft Active Directory, Samba 4 Active Directory)	—
Запуск службы прокси-сервер KSN на стороне точки распространения	✓	✓	—

Функция Агента администрирования	Windows	Linux	macOS
Загрузка обновлений через серверы обновлений "Лаборатории Касперского" в хранилища точек распространения, которые распространяют обновления на управляемые устройства	✓	✓	— Если устройства с операционной системой Linux или macOS находятся в области действия задачи Загрузка обновлений в хранилища точек распространения, задача завершится со статусом Сбой, даже если она успешно завершилась на всех устройствах с операционной системой Windows.
Принудительная установка приложений	✓	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой Linux.	С ограничением: невозможно выполнить принудительную установку на устройствах под управлением операционной системы Windows, используя точки распространения с операционной системой macOS.
Использовать в качестве push-сервера	✓	✓	—
Работа с приложениями сторонних производителей			
Удаленная установка приложений на устройства (см. стр. 247).	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Настройка обновлений операционной системы в политике Агента администрирования	✓	—	—
Просмотр информации об уязвимостях в приложениях	✓	—	—
Поиск уязвимостей в приложениях	✓	—	—
Обновления программного обеспечения	✓	—	—
Инвентаризация программного обеспечения, установленного на устройствах	✓	✓	—
Виртуальные машины			
Установка Агента администрирования на виртуальные машины (см. стр. 258).	✓	✓	✓
Оптимизация параметров для VDI (см. стр. 258).	✓	✓	✓
Поддержка динамических виртуальных машин (см. стр. 259).	✓	✓	✓
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. 260).	✓	✓	✓
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	✓	✓	✓

Функция Агента администрирования	Windows	Linux	macOS
Удаленное подключение к рабочему столу клиентского устройства	✓	—	✓ С помощью системы Virtual Network Computing (VNC).
Загрузка автономного инсталляционного пакета с помощью мастера переноса данных	✓	✓	✓

См. также:

Развертывание Агента администрирования и приложения безопасности 239

Сравнение параметров Агента администрирования по операционным системам

В таблице ниже показано, какие параметры Агента администрирования доступны в зависимости от операционной системы управляемого устройства, на котором установлен Агент администрирования.

Таблица 40. Параметры Агента администрирования: сравнение по операционным системам

Раздел Параметры	Windows	Linux	macOS
Общие	✓	✓	✓
Настройка событий	✓	✓	✓
Параметры	✓	✓ Доступны следующие параметры: • **Распространять файлы только через точки распространения** • **Максимальный размер очереди событий (МБ)** • **Приложение может получать расширенные данные политики на устройстве**	✓

Раздел Параметры	Windows	Linux	macOS
Хранилища	✓	✓ Доступны следующие параметры: • **Информация об установленных приложениях** • **Информация о реестре оборудования**	✓ Параметр **Сведения о реестре оборудования** доступен.
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: • **Сеть Windows** • **IP-диапазоны** • **Контроллеры домена**	✓ Доступны следующие параметры: • **Zeroconf** • **IP-диапазоны** • **Контроллеры домена**	—
Параметры сети для точек распространения	✓	✓	✓
Прокси-сервер KSN (точки распространения)	✓	✓	—
Обновления (точки распространения)	✓	✓	—

Раздел Параметры	Windows	Linux	macOS
История ревизий	✓	✓	✓

Включение и выключение режима низкого потребления ресурсов для Агента администрирования

Режим низкого потребления ресурсов позволяет ограничить использование оперативной памяти Агента администрирования, установленного на клиентском устройстве. По умолчанию режим низкого потребления ресурсов выключен.

В режиме низкого потребления ресурсов не выполняются следующие функции:

- Агент администрирования не может быть назначен точкой распространения (вручную или автоматически).
- Агент администрирования не записывает информацию о состоянии Агента администрирования в отдельный текстовый файл.
- Агент администрирования не поддерживает офлайн-модель получения обновлений.
- Следующие компоненты и процессы выключены:
  - Получение информации о сторонних обновлениях и уязвимостях.
  - Запуск прокси-сервера KSN на стороне точки распространения.
  - Загрузка обновлений в хранилище точки распространения.
  - Не использование блокировки DNS-сервера.

Компоненты и процессы возобновляют работу после выключения режима низкого потребления ресурсов.

► *Чтобы включить режим низкого потребления ресурсов:*

1. Выполните следующую команду в командной строке на клиентском устройстве:

   ```
   $ sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Перезапустите Агент администрирования с помощью следующей команды:

   ```
   $ sudo service klnagent64 restart
   ```

3. Проверьте, включен ли режим низкого потребления ресурсов, используя следующую команду:

   ```
   $ sudo service klnagent64 status
   ```

   Режим низкого потребления ресурсов включен.

► *Чтобы выключить режим низкого потребления ресурсов:*

1. Выполните следующую команду в командной строке на клиентском устройстве:

```
$ sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
KLNAG_FLAG_TEST_VM_PERF -t d -v 0
```

2. Перезапустите Агент администрирования с помощью следующей команды:

   ```
   $ sudo service klnagent64 restart
   ```

3. Проверьте, выключен ли режим низкого потребления ресурсов, используя следующую команду:

   ```
   $ sudo service klnagent64 status
   ```

   Режим низкого потребления ресурсов выключен.

Также можно включить режим низкого потребления ресурсов удаленно с помощью задачи *Удаленное выполнение скриптов* (см. стр. 363).

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:

Сценарий: настройка защиты сети.....393

В этом разделе

Настройка Kaspersky Security Network

Kaspersky Security Network (KSN) – инфраструктура облачных служб, обладающая информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network позволяет Kaspersky Endpoint Security для Windows быстрее реагировать на различные виды угроз, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний. Подробнее о Kaspersky Security Network см. документацию Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/ru-RU/176440.htm.

► *Чтобы задать рекомендуемые параметры KSN:*

1. В главном окне приложения 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 приложения** → **Продвинутая защита** → **Kaspersky Security Network**.
4. Убедитесь, что параметр **Использовать прокси-сервер KSN** включен. Использование этого параметра поможет перераспределить и оптимизировать трафик сети.

   Если вы используете Managed Detection and Response https://support.kaspersky.com/MDR/ru-RU/, вы должны включить параметр **Прокси-сервер KSN** (см. стр. 425) для точки распространения https://support.kaspersky.com/KESWin/12.3/ru-ru/126799.htm.
5. Если служба прокси-сервера KSN недоступна, можно включить использование серверов KSN. 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:

Сценарий: настройка защиты сети 393

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 приложения, 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/12.3/ru-RU/176738.htm.

► *Чтобы проверить список сетей:*

1. В главном окне приложения 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 приложения → 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.....393

Выключение проверки сетевых устройств

Проверка сетевых дисков приложением 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/12.3/ru-RU/176733.htm.

► *Чтобы выключить проверку сетевых дисков:*

1. В главном окне приложения 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 приложения → 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 393

kaspersky

Исключение сведений о программном обеспечении из памяти Сервера администрирования

Рекомендуется, настроить Сервер администрирования так, чтобы он не сохранял информацию о модулях приложений, 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 модулях приложений:*

1. В главном окне приложения 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 приложения → Общие параметры → Отчеты и хранилища**.**
4. В блоке **Информировать Сервер администрирования**, снимите флажок **О запускаемых приложениях**, если он установлен в политике верхнего уровня.

   Когда этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех модулей приложений на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center (десятки гигабайтов).

Информация об установленных модулях приложений больше не сохраняется в базе данных Сервера администрирования.

См. также:

Сценарий: настройка защиты сети 393

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/12.3/ru-RU/178492.htm.

► *Чтобы задать рекомендуемые параметры интерфейса:*

1. В главном окне приложения 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 приложения → 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 393

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 приложения 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 приложения выключен.*
   - *Ошибка активации.*
   - *Обнаружена активная угроза. Требуется запуск процедуры лечения.*
   - *Лечение невозможно.*
   - *Обнаружена ранее открытая опасная ссылка.*
   - *Процесс прерван.*
   - *Сетевая активность запрещена.*

- *Обнаружена сетевая атака.*
- *Запуск приложения 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 приложения.*

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 приложения 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 приложения.*
   - *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 приложения запрещен в тестовом режиме.*
11. Нажмите на кнопку **ОК**.

Регистрация важных событий в базе данных Сервера администрирования настроена.

См. также:

Сценарий: настройка защиты сети.....393

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.....393

kaspersky

Kaspersky Security Network и Kaspersky Private Security Network

В этом разделе описано использование инфраструктуры онлайн-служб Kaspersky Security Network (KSN) и Kaspersky Private Security Network (KPSN). Приведена информация о KSN и KPSN, а также инструкции по включению KPSN, настройке доступа к KPSN, по просмотру статистики использования прокси-сервера KSN.

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 приложений "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 приложениях, установленных на управляемых устройствах.

Участвуя в программе KSN, вы соглашаетесь в автоматическом режиме предоставлять в "Лабораторию Касперского" информацию о работе приложений "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. 446).

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. 446). 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.
- *Kaspersky Private Security Network (KPSN)* – это решение, которое предоставляет пользователям устройств с установленными приложениями "Лаборатории Касперского" доступ к базам данных Kaspersky Security Network и другим статистическим данным без отправки данных со своих устройств в KSN. 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 **Параметры прокси-сервера KSN** окна свойств Сервера администрирования (см. стр. 446).

Приложение предлагает присоединиться к KSN во время работы мастера первоначальной настройки (см. стр. 147). Вы можете начать использование KSN или отказаться от использования KSN в любой момент работы с приложением (см. стр. 448).

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, приложение использует публичные DNS-серверы (см. стр. 194). 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. 446).

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 приложения "Лаборатории Касперского":

   - Kaspersky Security Center
   - Kaspersky Endpoint Security для Linux
   - Kaspersky Endpoint Security для Windows

   Если вы включите KPSN в Kaspersky Security Center, эти приложения получат об этом информацию о поддержке KPSN. В окне свойств приложения 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 управляемого приложения 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.
   - Чтобы Сервер администрирования подключался к прокси-серверу KSN через HTTPS-порт, выберите параметр **Использовать HTTPS-порт** и в поле **HTTPS-порт** укажите номер порта. По умолчанию параметр выключен, используется порт TCP. Если параметр включен, по умолчанию подключение к прокси-серверу KSN выполняется через HTTPS-порт 17111.
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. 290).
2. В главном меню нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.
3. На вкладке **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, вам нужно 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) вам нужно 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.

Принятие обновленного Положения о KSN

Вы используете KSN в соответствии с Положением о KSN, которое вы читаете и принимаете при включении KSN (см. стр. 449). 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 приложения.

   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. 449) 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 приложения** → **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.

В сертифицированной версии программы использование Глобального KSN не допускается, так как приводит к выходу программы из сертифицированного состояния.

kaspersky

Управление задачами

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

В этом разделе

См. также:

Сценарий: настройка защиты сети 393

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 приложений, проверка файлов, обновление баз и модулей приложений, другие действия с приложениями.

Вы можете создать задачу для приложения в Kaspersky Security Center Web Console, только если для этого приложения 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 приложения 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 каждого приложения 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 запущено приложение, для которого 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. 452) – 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 для выборок устройств 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 452

Создание задачи

► *Чтобы создать задачу:*

1. В главном окне приложения перейдите к вкладке **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.

► *Чтобы создать задачу, назначенную выбранным устройствам:*

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

   Отобразится список управляемых устройств.

2. В списке управляемых устройств установите флажки рядом с устройствами, для которых нужно запустить задачу. Вы можете использовать функции поиска и фильтрации, чтобы найти необходимые устройства.
3. Нажмите на кнопку **Запустить задачу** и выберите **Создать задачу**.

   Запустится мастер создания задачи.

   На первом шаге мастера вы можете удалить устройства, выбранные для включения в область действия задачи. Следуйте инструкциям мастера.
4. Нажмите на кнопку **Готово**.

Задача создана для выбранных устройств.

См. также:

Управление задачами 452
Общие параметры задач 456
Сценарий: развертывание приложений "Лаборатории Касперского" 333
Сценарий: мониторинг и отчеты 544
Сценарий: настройка защиты сети 393

Запуск задачи вручную.

Приложение запускает задачи в соответствии с расписанием, заданным в свойствах каждой задачи. Вы можете запустить задачу вручную в любое время из списка задач. Также можно выбрать устройства в списке **Управляемые устройства** и запустить для них существующую задачу.

► *Чтобы запустить задачу вручную:*

1. В главном окне приложения перейдите к вкладке **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:

О задачах 452
Создание задачи 454
Общие параметры задач 456
Сценарий: настройка защиты сети 393

kaspersky

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center.

► *Чтобы просмотреть список задач,*

В главном окне приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям приложений, к которыми они относятся. Например, задача *Удаленная установка приложения* 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 вкладками (см. стр. 456). Например, **Тип задачи** отображается на вкладке **Общие**, а расписание задачи на вкладке **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 приложения в заблокированных сеансах**

    Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

    Если этот параметр включен, такие приложения 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 приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

- Параметры расписания задачи:
  - **Параметры запуска задачи:**
    - **Каждый N час**

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые 6 часов, начиная с текущих системной даты и времени.

    - **Каждые N дней**

      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 приложением, для которого 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 каждую пятницу в текущее системное время.

    - **Каждые 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 выбран этот вариант.

- **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.

- **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. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

  - **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 приложения "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. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой

задачи, которую вы хотите запустить только вне рабочих часов.

По умолчанию параметр выключен.

- **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 автоматическую случайную задержку запуска задачи в интервале**

  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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.

  - **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**

  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 было установлено и запущено приложение, выполняющее 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:
  - **Распространить на подгруппы**
  - **Распространить на подчиненные и виртуальные Серверы администрирования**
- Дополнительные параметры расписания:
  - **Включать устройства перед запуском задачи функцией Wake-on-LAN за**

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**

  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 приложения, 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 приложения, 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 приложения, 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.

  - **выборкам 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 приложений "Лаборатории Касперского" 333

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. 463).

► *Чтобы экспортировать задачу:*

1. В главном окне приложения перейдите к вкладке **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 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. 462) и ее параметры.

► *Чтобы импортировать задачу:*

1. В главном окне приложения перейдите к вкладке **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**

     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 определенное приложение на устройства бухгалтеров или проверять устройства в подсети, которое, вероятно, заражено.
   - **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 приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

В этом разделе

См. также:

kaspersky

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**.

► *Чтобы просмотреть результаты задачи для подчиненного Сервера администрирования:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты откройте** окно **Результаты выполнения задачи**.
3. Нажмите на **Статистика подчиненного Сервера**.
4. Выберите подчиненный Сервер, для которого вы хотите отобразить окно **Результаты выполнения задачи**.

См. также:

kaspersky

Теги приложений

В этом разделе описаны теги приложений, приведены инструкции по их созданию и изменению, а также по назначению тегов сторонним приложениям.

В этом разделе

См. также:

О тегах приложений

Kaspersky Security Center позволяет назначать теги сторонним приложениям (приложениям, выпущенным производителями, отличными от "Лаборатории Касперского"). Тег представляет собой метку приложения, которую можно использовать для группировки и поиска приложений. Назначенный приложению тег можно использовать в условиях для выборок устройств (см. стр. 304).

Например, можно создать тег `[Браузеры]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

См. также:

Создание тегов приложений

► *Чтобы создать тег приложения:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
2. Нажмите на кнопку **Добавить**.

Отобразится окно создания тега.

3. Укажите тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Созданный тег появляется в списке тегов приложения.

См. также:

Сценарий: управление приложениями 654
Сценарий: обнаружение сетевых устройств 198

Изменение тегов приложений

► *Чтобы переименовать тег приложения:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Теги приложений**.
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 приложений.

См. также:

Сценарий: управление приложениями 654
Сценарий: обнаружение сетевых устройств 198

Назначение тегов приложениям

► *Чтобы назначить приложению теги:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Выберите приложение, для которого требуется назначить теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, 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 приложению.

См. также:

Сценарий: управление приложениями 654
Сценарий: обнаружение сетевых устройств 198

Снятие назначенных тегов с приложений

► *Чтобы снять теги с приложения:*

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Реестр приложений**.
2. Выберите приложение, с которого требуется снять теги.
3. Выберите вкладку **Теги**.

   На вкладке появятся все теги приложений, существующие на Сервере администрирования. Теги, назначенные выбранному приложению, 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 приложения.

Снятые с приложений теги не удаляются. При необходимости их можно удалить вручную (см. стр. 469).

См. также:

Сценарий: управление приложениями 654
Сценарий: обнаружение сетевых устройств 198

Удаление тегов приложений

► *Чтобы удалить тег приложения:*

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Теги приложений**.
2. В списке выберите теги приложения, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Выбранный тег приложения удален. Удаленный тег автоматически снимается со всех приложений, которым он был назначен.

См. также:

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.

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 приложения → 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 приложения 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 приложения** 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 393

Использование утилиты klscflag для открытия порта 13291

Если вы хотите использовать утилиту klakaut, откройте порт 13291 с помощью утилиты klscflag.

Утилита изменяет значение параметра KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

► *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_SETTINGS\";"
```

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 приложением Kaspersky Security Center Web Console 48

Порты, используемые Kaspersky Security Center 42

Регистрация приложения Kaspersky Industrial CyberSecurity for Networks в Kaspersky Security Center Web Console

Чтобы начать работу с приложением Kaspersky Industrial CyberSecurity for Networks через Kaspersky Security Center Web Console, необходимо предварительно зарегистрировать его в Kaspersky Security Center Web Console.

► *Чтобы зарегистрировать приложение Kaspersky Industrial CyberSecurity for Networks:*

1. Убедитесь, что сделано следующее:
   - Вы загрузили и установили веб-плагин Kaspersky Industrial CyberSecurity for Networks (см. стр. 335).

     Можно сделать это позже, ожидая синхронизацию Сервера Kaspersky Industrial CyberSecurity for Networks с Сервером администрирования. После загрузки и установки плагина в главном меню Kaspersky Security Center Web Console отображается раздел **KICS for Networks**.
   - В веб-интерфейсе Kaspersky Industrial CyberSecurity for Networks настраивается и включается взаимодействие с Kaspersky Security Center. Подробную информацию см. в справке Kaspersky Industrial CyberSecurity for Networks.
2. Переместите устройство, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks, из группы Нераспределенные устройства в группу Управляемые устройства:
   a. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Обнаружение устройств** → **Контроллеры доменов**.

b. Установите флажок рядом с устройством, на котором установлен Kaspersky Industrial CyberSecurity for Networks Server.

c. Нажмите на кнопку **Переместить в группу**.

d. В иерархии групп администрирования установите флажок рядом с группой **Управляемые устройства**.

e. Нажмите на кнопку **Переместить**.

3. Откройте окно свойств устройства, на котором установлен Сервер Kaspersky Industrial CyberSecurity for Networks.
4. На странице свойств устройства в разделе **Общие**, выберите параметр **Не разрывать соединение с Сервером администрирования**, а затем нажмите на кнопку **Сохранить**.
5. В окне свойств устройства выберите раздел **Приложения**.
6. В разделе **Приложения** выберите Агент администрирования Kaspersky Security Center Network.
7. Если текущий статус приложения *Остановлено*, подождите, пока он не изменится на *Выполняется*.

   Это может занять до 15 минут. Если вы еще не установили веб-плагин Kaspersky Industrial CyberSecurity for Networks, вы можете сделать это сейчас.
8. Если вы хотите просматривать статистику работы Kaspersky Industrial CyberSecurity for Networks, вы можете добавить веб-виджеты в панель управления. Чтобы добавить веб-виджеты, выполните следующее:

   a. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.

   b. В панели управления нажмите на кнопку **Добавить или восстановить веб-виджет**.

   c. В появившемся веб-виджете нажмите на кнопку **Другое**.

   d. Выберите веб-виджет, который вы хотите добавить.

      - Карта размещения KICS for Networks
      - Информация о Серверах KICS for Networks
      - Актуальные события KICS for Networks
      - Устройства, требующие внимания в KICS for Networks
      - Критические события KICS for Networks
      - Статусы KICS for Networks
9. Чтобы перейти в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks, выполните следующие действия:

   a. В главном окне приложения перейдите в раздел **KICS for Networks → Поиск**.

   b. Нажмите на кнопку **Найти события или устройства**.

   c. В открывшемся окне **Параметры запроса** нажмите на поле **Сервер**.

   d. В раскрывающемся списке серверов, интегрированных с Kaspersky Security Center, выберите Сервер Kaspersky Industrial CyberSecurity for Networks и нажмите на кнопку **Найти**.

   e. Перейдите по ссылке **Перейти на Сервер** рядом с названием Сервера Kaspersky Industrial CyberSecurity for Networks.

      Откроется страница входа в Kaspersky Industrial CyberSecurity for Networks.

Для входа в веб-интерфейс Kaspersky Industrial CyberSecurity for Networks вам необходимо ввести учетные данные пользователя приложения.

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:

Об учетных записях пользователей

Kaspersky Security Center позволяет управлять учетными записями пользователей и группами

безопасности. Приложение 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 приложения 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 приложений "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. 488).

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.

Отличия от использования профилей политики

Профили политики – это свойства политики, созданной для каждого приложения "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных приложений. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

См. также:

Сценарий: настройка защиты сети.....393

kaspersky

Настройка прав доступа к функциям приложения Управление доступом на основе ролей

Kaspersky Security Center предоставляет доступ на основе ролей к функциям Kaspersky Security Center и к функциям управляемых приложений «Лаборатории Касперского».

Вы можете настроить права доступа к функциям приложения (см. стр. 478) для пользователей Kaspersky Security Center одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей (см. стр. 476) 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 приложению. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В приложении можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли (см. стр. 485) пользователей с уже настроенным набором прав или создавать роли (см. стр. 511) и самостоятельно настраивать необходимые права.

В этом разделе

См. также:

Сценарий: настройка защиты сети 393

Права доступа к функциям приложения

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.

Функциональная область **Общие функции**: **Доступ к объектам независимо от их списков ACL** предназначена для аудита. Когда пользователям предоставляется право **Чтение** в этой функциональной области, они получают полный доступ на **Чтение** ко всем объектам и могут выполнять любые созданные задачи на выбранных устройствах, подключенных к Серверу администрирования через Агент администрирования с правами локального администратора (root для Linux). Рекомендуется предоставлять эти права ограниченному кругу пользователей, которым они нужны для выполнения своих служебных обязанностей.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общий функционал: Базовая функциональность**.

Таблица 41. Права доступа к функциям приложения

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.	Доступ предоставляется независимо от других прав, даже если они запрещают доступ на чтение к определенным объектам.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
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**. • Просмотр журнала операционной системы: **Чтение**.	• Загрузка обновлений в хранилище Сервера администрирования. • Рассылка отчетов. • Распространение инсталляционных пакетов. • Установка приложений 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 приложениях для защиты почтовых систем. • Сводный отчет о приложениях для защиты рабочих станций и файловых серверов. • Сводный отчет о приложениях для защиты периметра. • Сводный отчет о типах установленных приложений. • 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 об уязвимостях. • Отчет о запрещенных приложениях. • 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 к зашифрованным файлам. • Отчет об эффективных правах пользователя. • Отчет о правах.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
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.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
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**. • 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**.	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.	Отсутствует.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Общие функции: **Развертывание приложений "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 приложений "Лаборатории Касперского". • Отчет о несовместимых приложениях. • Отчет о версиях обновлений модулей приложений "Лаборатории Касперского". • Отчет о развертывании защиты.	Инсталляционный пакет: "Лаборатория Касперского".
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 ACL объекта**. • Управление ролями пользователей: **Изменение списков ACL объекта**. • Управление внутренними пользователями: **Изменение списков ACL объекта**. • Управление группами безопасности: **Изменение списков ACL объекта**. • Управление псевдонимами: **Изменение списков управления доступом объектов.**	Отсутствует.	Отсутствует.	Отсутствует.
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.

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет	Другое
Управление системой: **Системное администрирование**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Просмотр свойства патчей сторонних производителей: **Чтение**. • Изменение свойства патчей сторонних производителей: **Запись**.	• Закрытие уязвимостей. • Установка требуемых обновлений и закрытия уязвимостей.	Отчет об обновлениях ПО.	Отсутствует.
Управление системой: **Удаленное выполнение скриптов**	• **Чтение.** • **Запись.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Пользователь может просматривать свойства задачи: **Чтение**. Пользователь может создать, удалить или изменить инсталляционный пакет: **Запись**. Пользователь может запустить задачу или запланировать ее запуск: **Выполнение**. Пользователь может запустить задачу на выбранных устройствах: **Выполнение действий над выборками устройств**.	"Удаленное выполнение скриптов"	Отсутствует.	Отсутствует.

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center, предоставляют им набор прав доступа к функциям приложения.

Пользователям, которые были созданы на виртуальном Сервере, невозможно назначить роли на Сервере администрирования.

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 42. 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.

Роль	Комментарий
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 43. 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.**
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.

Роль	Описание
Администратор установки приложений	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание приложений "Лаборатории Касперского".** • **Управление лицензионными ключами.** Предоставляет права на **Чтение** и **Выполнение в следующей** функциональной области **Базовая функциональность: Виртуальные Серверы администрирования.**
Оператор установки приложений	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание приложений "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области)**.** • **Виртуальные Серверы администрирования.**
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общие функции: Базовая функциональность.** • 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: • **Общие функции: Базовая функциональность.** • Область Kaspersky Endpoint Security, включая все функции.
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 приложений "Лаборатории Касперского".**
	  • **Виртуальные Серверы администрирования.**
	• Область Kaspersky Endpoint Security, включая все функции.

Роль	Описание
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 приложения 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.

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. 478). Приложение 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. 476), 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 приложений "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 безопасности, которым нужно назначить права, а затем нажмите на кнопку **Права доступа**.

   Вы не можете выбрать несколько пользователей или групп безопасности 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 другого приложения "Лаборатории Касперского".

   b. Установите флажок **Разрешить** или **Запретить** рядом с нужной функцией или правом доступа.

      Пример 1: Установите флажок **Разрешить** рядом с узлом **Интеграции приложения**, чтобы предоставить пользователю или группе все доступные права доступа к функции интеграции приложения (**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.
  - Доступ к объектам независимо от их списков ACL.
  - Базовая функциональность.
  - Удаленные объекты.
  - Управление ключами шифрования.
  - Обработка событий.
  - Операции с Сервером администрирования (только в окне свойств Сервера администрирования).
  - Развертывание приложений "Лаборатории Касперского".
  - Управление лицензионными ключами.
  - Интеграция приложений.
  - Управление отчетами.
  - 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.
  - Удаленная установка.
  - Инвентаризация приложений.

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 приложения 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 256 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. 510).
> 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.

Учетная запись пользователей добавлена в список пользователей.

См. также:

Сценарий: настройка защиты сети 393

Создание группы безопасности

► *Чтобы создать группу безопасности:*

1. В главном окне приложения 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.

Группа безопасности добавлена в список групп.

См. также:

Сценарий: настройка защиты сети 393

kaspersky

Изменение учетной записи внутреннего пользователя

► *Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center:*

1. В главном окне приложения 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 вкладке **Общие** измените параметры учетной записи пользователя:
   - **Описание.**
   - **Полное имя.**
   - **Адрес электронной почты.**
   - **Основной телефон.**
   - **Задать новый пароль** для подключения пользователя к Kaspersky Security Center.

     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 256 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. 510) 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 приложению. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.
4. На вкладке **Дополнительные настройки безопасности** вы можете указать параметры безопасности для этой учетной записи.
5. На вкладке **Группы** можно добавить пользователя или группу безопасности.
6. На вкладке **Устройства** можно назначить устройства пользователю (см. стр. 496).
7. На вкладке **Роли** можно назначить роль пользователю (см. стр. 512).
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей.

См. также:

Сценарий: настройка защиты сети 393

Изменение группы безопасности

► *Чтобы изменить группу безопасности:*

1. В главном окне приложения 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. 495). Эти параметры доступны только для внутренних пользователей и внутренних групп безопасности.
   - На вкладке **Роли** можно назначить роль группе безопасности (см. стр. 494).
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Изменения применены к группе безопасности.

См. также:

Сценарий: настройка защиты сети 393

Назначение роли пользователю или группе безопасности

► *Чтобы назначить роли пользователю или группе безопасности:*

1. В главном окне приложения 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 для работы с Сервером администрирования будет назначена пользователю (или пользователям, или группе безопасности). В списке пользователей или групп безопасности 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 в группу безопасности:*

1. В главном окне приложения 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. 494).

См. также:

Сценарий: настройка защиты сети.....393

kaspersky

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 приложения 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 вкладку **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**.

В этом разделе

См. также:

Сценарий: настройка защиты сети 393

kaspersky

Назначение пользователя владельцем устройства при установке Агента администрирования

Чтобы назначить пользователя владельцем устройства при установке Агента администрирования с помощью инсталляционного пакета, добавьте в параметры инсталляционного пакета Агента администрирования переменные, указанные в таблице ниже.

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Нет	Позволяет запустить утилиту для регистрации пользователя в качестве владельца устройства после установки Агента администрирования. Если выключено, то регистрация в качестве владельца устройства недоступна для пользователя.	1 – утилита для регистрации пользователя в качестве владельца устройства запустится после установки Агента администрирования. Другое – утилита недоступна.
KLNAGENT_DEVICEOWNER_LOGIN	Нет Да, если ввести пароль	Содержит учетную запись пользователя, который будет зарегистрирован как владелец устройства.	Учетная запись пользователя, который указан в списке пользователей в Kaspersky Security Center.
KLNAGENT_DEVICEOWNER_PASSWORD	Нет Да, если ввести учетную запись	Содержит зашифрованный пароль пользователя, который будет зарегистрирован как владелец устройства.	Пароль пользователя.

Агент администрирования расшифрует указанные учетную запись и пароль при установке Kaspersky Security Center, и пользователь будет зарегистрирован как владелец устройства.

Вы также можете назначить пользователя владельцем устройства при установке Агента администрирования в тихом режиме с файлом ответов. Подробнее об установке в тихом режиме с помощью файла ответов см. статью (см. стр. 250).

► *Чтобы назначить пользователя владельцем устройства при установке Агента администрирования в тихом режиме с файлом ответов:*

1. Добавьте параметр KLNAGENT_DEVICEOWNER_REGISTRATION_START в файл ответов и установите для него значение 1.

   Утилита для регистрации пользователя в качестве владельца устройства запустится после установки Агента администрирования.

2. Введите учетную запись и пароль в командной строке на клиентском устройстве.

   Пользователь назначен владельцем устройства.

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Если для пользователя включена двухэтапная проверка, вам необходимо ввести временный одноразовый пароль (TOTP) из приложения. Подробнее о двухэтапной проверке см. статью (см. стр. 499).

Назначение пользователя владельцем устройства после установки Агента администрирования

► *Чтобы разрешить пользователю регистрироваться в качестве владельца устройства:*

1. В Kaspersky Security Center Web Console перейдите в раздел **Обнаружение и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.

   Откроется список инсталляционных пакетов.

2. Нажмите на инсталляционный пакет Агента администрирования.

   Отобразится окно свойств инсталляционного пакета.

3. В открывшемся окне свойств инсталляционного пакета перейдите на вкладку **Параметры** → **Дополнительно**.

4. В разделе **Регистрация пользователя в качестве владельца устройства (только для Linux)** включите параметр **Разрешить запуск утилиты регистрации пользователей после установки Агента администрирования** и нажмите на кнопку **Сохранить**.

Утилиту для регистрации пользователя в качестве владельца устройства можно запустить из командной строки на клиентском устройстве.

► *Чтобы зарегистрировать пользователя в качестве владельца устройства на клиентском устройстве:*

1. Выполните следующую команду в командной строке на клиентском устройстве:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Если потребуется, введите учетную запись и пароль.

   Если учетная запись и пароль включены в файл ответов или инсталляционный пакет Агента администрирования, выполните следующую команду в командной строке на клиентском устройстве:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Если для пользователя включена двухэтапная проверка, вам необходимо ввести временный одноразовый пароль (TOTP) из приложения. Подробнее о двухэтапной проверке см. статью (см. стр. 499).

Пользователь зарегистрирован как владелец устройства.

Отмена назначения пользователя владельцем устройства

► *Чтобы отменить назначение пользователя в качестве владельца устройства на клиентском устройстве:*

1. Выполните следующую команду в командной строке на клиентском устройстве:
   `$ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner`
2. Введите имя пользователя и пароль.

Если пользователь входит во внутреннюю группу безопасности, учетная запись должна содержать имя пользователя.

Если пользователь входит в группу безопасности Active Directory, учетная запись должна содержать имя пользователя и имя домена.

Если для пользователя включена двухэтапная проверка, вам необходимо ввести временный одноразовый пароль (TOTP) из приложения. Подробнее о двухэтапной проверке см. статью (см. стр. 499).

Назначение пользователя владельцем устройства отменено.

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 приложения 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 вкладку **Дополнительные настройки безопасности**.
4. На вкладке **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, приложение 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 для аутентификации.

Этапы

Включение двухэтапной проверки для всех пользователей состоит из следующих этапов:

1. Установка приложения для аутентификации 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 для аутентификации, 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 для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

ii. Синхронизация времени приложения для аутентификации и время устройства, на котором установлен Сервер администрирования

Убедитесь, что время на устройстве с приложением для аутентификации и время на устройстве с Сервером администрирования синхронизированы с UTC с помощью внешних источников времени. Иначе возможны сбои при аутентификации и активации двухэтапной проверки.

jj. Включение двухэтапной проверки и получение секретного ключа для своей учетной записи

После включения двухэтапной проверки для своей учетной записи (см. стр. 504) вы можете включить двухэтапную проверку для всех пользователей.

kk. Включение двухэтапной проверки для всех пользователей

Пользователи с включенной двухэтапной проверкой (см. стр. 505) должны использовать ее для входа на Сервер администрирования.

ll. 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. 508).

mm. Изменение имени издателя кода безопасности

Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности (см. стр. 509) для лучшего распознавания разных Серверов администрирования.

nn. Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку

При необходимости исключите учетные записи пользователей из двухэтапной проверки (см. стр. 507). Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

oo. 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. 507). 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, вам нужно установить приложение для аутентификации 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 для аутентификации. 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 для аутентификации. Если вы изменили имя издателя кода безопасности, необходимо выпустить новый секретный ключ и передать его приложению для аутентификации. 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 приложение, 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 для аутентификации. Например, Google Authenticator. Чтобы сгенерировать код безопасности, вам нужно синхронизировать время, установленное в приложении для аутентификации, со временем, установленным для Сервера администрирования.

Чтобы проверить, поддерживает ли Kaspersky Security Center приложение для аутентификации, 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 для аутентификации. В случае успеха Kaspersky Security Center поддерживает выбранное приложение проверки подлинности.

Приложение для аутентификации 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 для аутентификации.
3. Приложение для аутентификации генерирует одноразовый код безопасности, который вы передаете в окно аутентификации Сервера администрирования.

Рекомендуется установить приложение для аутентификации 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. 507) 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. 235).

См. также:

Включение двухэтапной проверки для вашей учетной записи 504

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 для аутентификации. Убедитесь, что время, установленное в приложении для аутентификации, синхронизировано со временем устройства, на котором установлен Сервер администрирования.

► *Чтобы включить двухэтапную проверку для учетной записи пользователя:*

1. В главном окне приложения 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 500

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 вкладке **Дополнительные настройки безопасности** окна свойств включите **двухэтапную проверку для всех пользователей**.

3. Если вы не включили двухэтапную проверку для своей учетной записи, приложение откроет окно включения двухэтапной проверки для вашей учетной записи (см. стр. 504).

   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. 507) из двухэтапной проверки.

См. также:

Сценарий: настройка двухэтапной проверки для всех пользователей 500

kaspersky

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 приложения 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 вкладку **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 500

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. 504) 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 вкладке **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 500

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 **Общие функции: Права пользователя**.

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 вкладке **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 500

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 для аутентификации. Убедитесь, что время на устройстве с приложением для аутентификации 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 для аутентификации на мобильном устройстве. Для этого выполните одно из следующих действий:
   - Введите секретный ключ в приложение для аутентификации 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 Kaspersky Security Center 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. 505).

► *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. 507).

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 приложения 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 вкладку **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 для аутентификации.
6. Нажмите на кнопку **Проверить и применить**.

Новый секретный ключ для пользователя создан.

Если вы потеряете свое мобильное устройство, можно установить приложение для аутентификации 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 для аутентификации.

► *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 вкладку **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 500

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 устройстве, на котором установлен Сервер 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 приложения 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 393

Создание роли пользователя

► *Чтобы создать роль пользователя:*

1. В главном окне приложения 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 вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью (см. стр. 512).
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

См. также:

Сценарий: настройка защиты сети 393

Изменение роли пользователя

► *Чтобы изменить роль пользователя:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.

3. В открывшемся окне измените параметры роли:
   - На вкладке **Общие** измените имя роли.

     Вы не можете изменять имена предопределенных ролей.
   - На вкладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью (см. стр. 512).
   - На вкладке **Права доступа** измените права доступа к приложениям "Лаборатории и Касперского".
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

См. также:

Сценарий: настройка защиты сети 393

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 приложения 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 шаге **Выбор роли** выберите роль, которую требуется назначить.
5. На шаге **Определение области** 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 приложения перейдите в раздел **Пользователи и роли** → **Роли**.

2. Выберите роль, для которой требуется задать область.
3. В открывшемся окне свойств роли перейдите на вкладку **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 шаге **Определение области** выберите группу администрирования, которую требуется добавить в область роли.
6. На шаге **Выбор пользователей** 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 393

Удаление роли пользователя

► *Чтобы удалить роль пользователя:*

1. В главном окне приложения 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 393

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 приложений городской навигации для всех устройств группы администрирования. Приложения 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. 476) владельцу этого устройства и создать профиль политики, разрешающий использовать приложения городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать приложения городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать приложения городской навигации на устройстве, принадлежащем вашей организации. Однако использование приложений городской навигации будет запрещено на других устройствах этой группы администрирования.

► *Чтобы связать роль с профилем политики:*

1. В главном окне приложения перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на вкладке **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 393

Обновление баз и приложений "Лаборатории Касперского"

Установка обновлений исполняемых модулей приложений "Лаборатории Касперского", не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу приложения из сертифицированного состояния.

В этом разделе описаны шаги, которые вам нужно выполнить для регулярных обновлений:

- баз и модулей приложений "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

В этом разделе

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, модулей приложений и приложений "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации (см. стр. 393), 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 модулей приложений "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 приложения 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, приложений "Лаборатории Касперского" и модулей приложений вручную (см. стр. 541) или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты приложения безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания приложений "Лаборатории Касперского" с помощью Kaspersky Security Center Web Console (см. стр. 333).
2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети (см. стр. 393).
3. Назначено соответствующее количество точек распространения (см. стр. 234) в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и приложений «Лаборатории Касперского» состоит из следующих этапов:

1. Выбор схемы обновления

   Есть несколько схем (см. стр. 518), которые вы можете использовать для установки обновлений для приложений безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

2. **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. 524).

3. **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. 530).

4. **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.

5. **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. 539). Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или модулей приложений "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или модулями приложения. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

   Инструкция: Использование файлов различий для обновления баз и модулей приложений "Лаборатории Касперского" (см. стр. 539)

6. **Настройка автоматической установки обновлений для приложений безопасности**

   Создайте задачу *Обновление* для управляемых приложений, чтобы обеспечить своевременное обновление модулей приложений 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. 456).

   Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять приложения 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.

7. **Одобрение и отклонение обновлений управляемых приложений "Лаборатории Касперского"**

По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус обновления на *Одобрено* или *Отклонено*. Одобренные обновления всегда устанавливаются. Если обновление управляемого приложения "Лаборатории Касперского" требует принять условия Лицензионного соглашения, сначала вам нужно прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства. Обновления, которым вы установили статус *Отклонено*, не устанавливаются на управляемые устройства. Если ранее отклоненное обновление для управляемого приложения было установлено, Kaspersky Security Center попытается удалить обновления со всех устройств.

Одобрение и отклонение обновлений доступно только для управляемых приложений "Лаборатории Касперского", установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается.

Инструкция: Одобрение и отклонение обновлений программного обеспечения (см. стр. 536).

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, модулей приложений и приложений "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вам нужно своевременно предоставлять обновления следующего:

- Баз и модулей приложений "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, приложение использует публичные DNS-серверы (см. стр. 194). 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 позволяет автоматически обновлять Агент администрирования и приложения "Лаборатории Касперского", установленные на клиентских устройствах под управлением Windows (см. стр. 536). Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" https://www.kaspersky.ru/small-to-medium-business-security и установить их вручную.

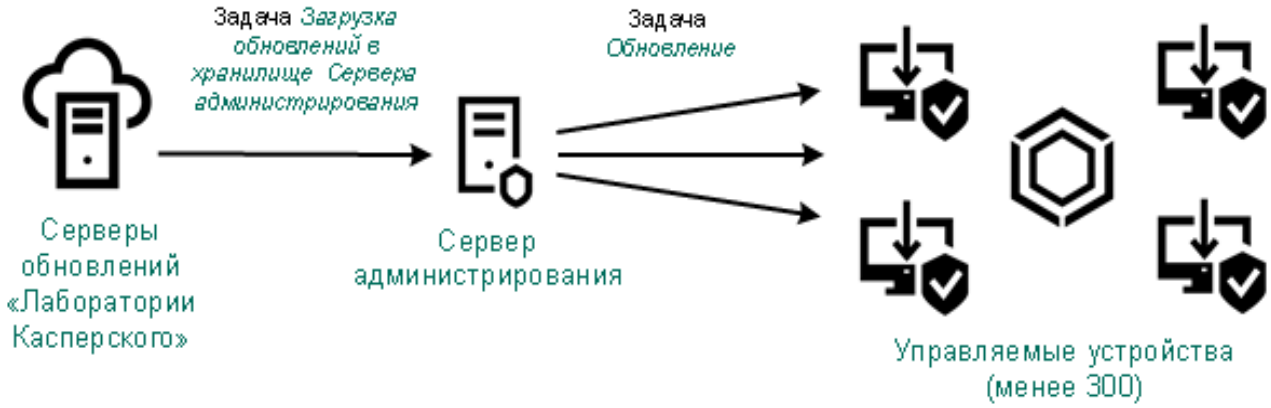
В зависимости от конфигурации вашей сети вы можете использовать следующие схемы загрузки и распространения необходимых обновлений на управляемые устройства:

- 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).



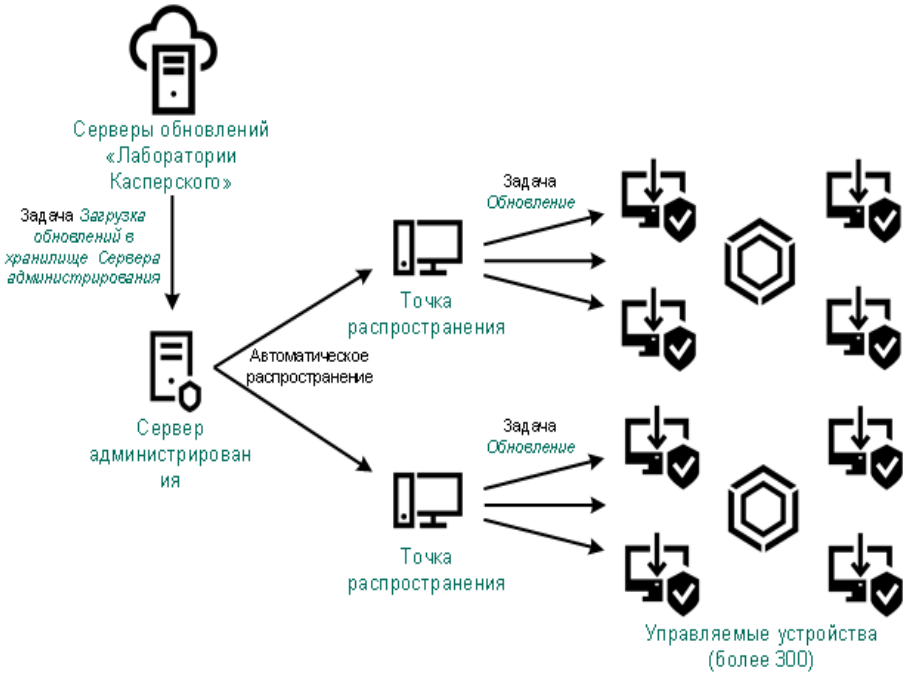
В качестве источника обновлений (см. стр. 535) можно использовать не только серверы обновлений "Лаборатории Касперского", но и локальную или сетевую папку.

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. 233) 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. 234) 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 модули приложения 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.

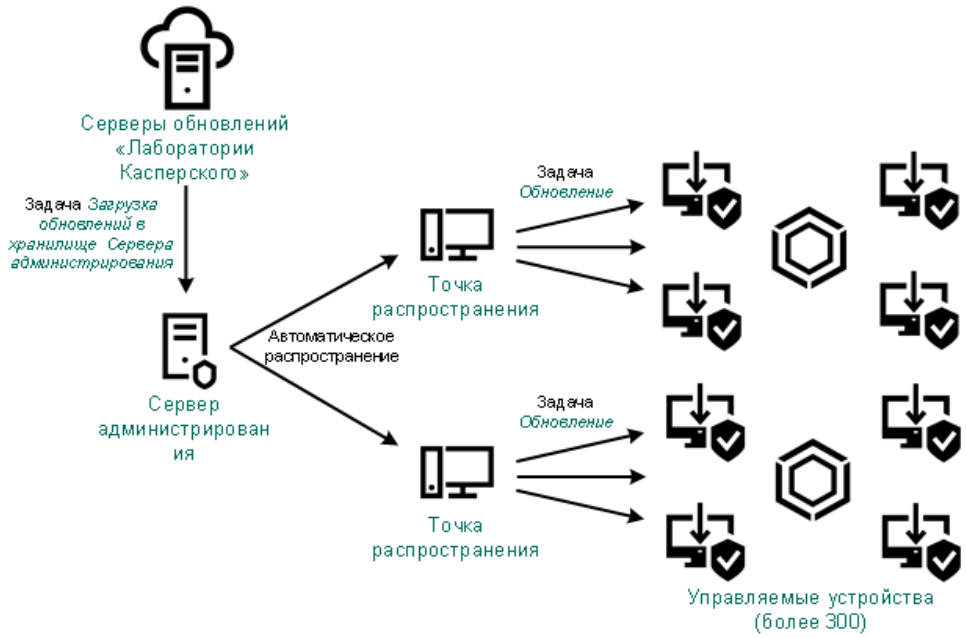
Каждое управляемое приложение "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются приложениями. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и модулей приложений "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия приложения;
- идентификатор установки приложения;
- 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.



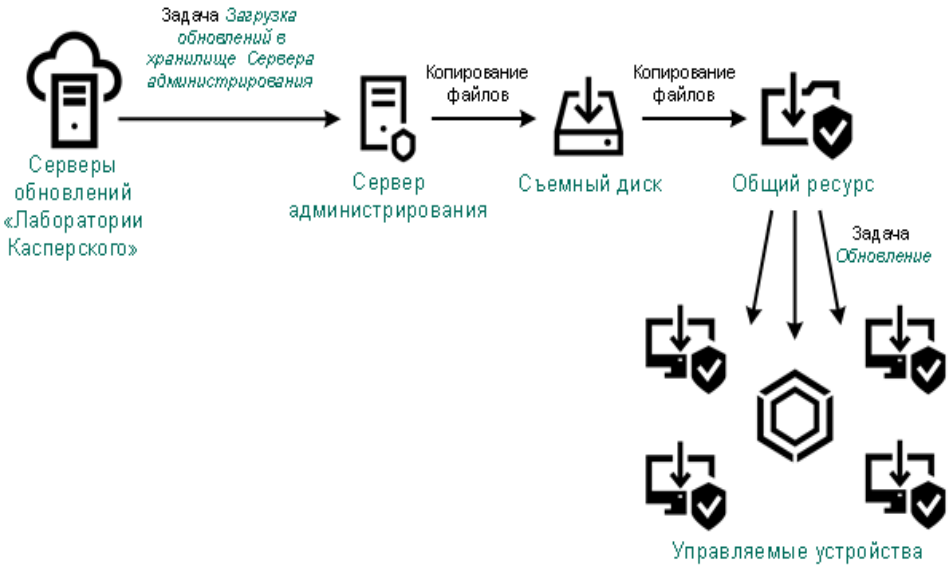
По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

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 модулей приложений "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, модулей приложений "Лаборатории Касперского" (см. стр. 541). 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).

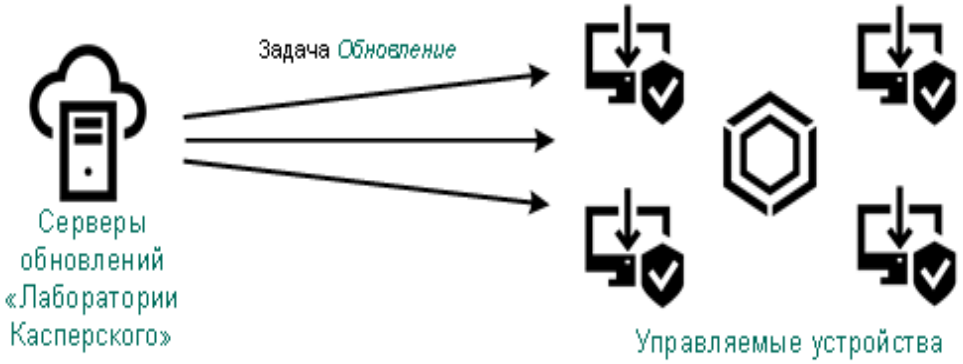


Подробнее об источниках обновлений в Kaspersky Endpoint Security см. в следующих справках:

- Справка Kaspersky Endpoint Security для Linux
- 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 приложении безопасности. Дополнительные сведения об этих параметрах см. в следующих разделах справки:

- Справка Kaspersky Endpoint Security для Linux
- Справка Kaspersky Endpoint Security для Windows

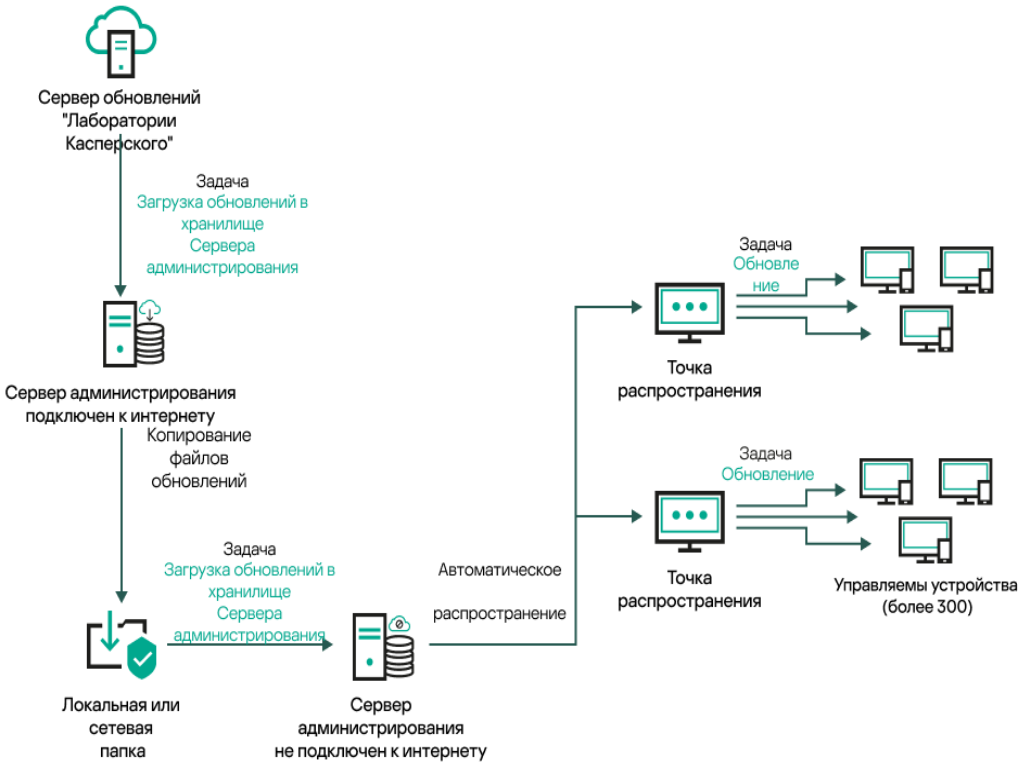
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

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 приложениями безопасности, наборы приложений 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. 524).



- 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. 524).

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....515

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и модулей приложения 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. 149). 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. 529). 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:*

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

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения 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 вкладке **Параметры приложения** 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. 535).

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 смонтируйте 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**
- **Принудительно обновить подчиненные Серверы**

  Если параметр включен, 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. 539).

  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. 529). 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 вкладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

    - **Запуск задачи**:

        - **Вручную** (выбрано по умолчанию)

Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию выбран этот вариант.

- **Каждые 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 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  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 приложением, для которого 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 каждую пятницу 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.

- **По завершении другой задачи**

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.
  - 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 приложения "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. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

      По умолчанию параметр выключен.

- **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 автоматическую случайную задержку запуска задачи в интервале**

  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**

  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 модулей приложений 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 приложений "Лаборатории Касперского".....515

kaspersky

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 приложения безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования приложения "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. 274). 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 какого-нибудь приложения, которое поддерживает Kaspersky Security Center, например, Kaspersky Endpoint Security для Linux (см .стр. 454). 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. 524).

► *Чтобы Kaspersky Security Center проверял полученные обновления перед распространением их на клиентские устройства:*

1. В главном окне приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.

2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на вкладку **Параметры приложения** 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 приложений "Лаборатории Касперского".....515

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 модулей приложений для приложений безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления приложений безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

► *Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

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

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения 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 вкладке **Параметры приложения** 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 приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

  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. В качестве сетевой папки можно использовать только смонтированную общую папку SMB. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

> 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 смонтируйте 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. 539).

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

1. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск задачи**:
  - **Вручную** (выбрано по умолчанию)

Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию выбран этот вариант.

- **Каждые 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 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  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 приложением, для которого 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 каждую пятницу 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.

- **При обнаружении вирусной атаки**

  Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы приложений.

  Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление*

устройствами с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.
  - **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 приложения "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. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

    По умолчанию параметр выключен.
  - **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 автоматическую случайную задержку запуска задачи в интервале**

    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 приложений "Лаборатории Касперского".....515

Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования

При создании или использовании задачи загрузки обновлений в хранилище Сервера администрирования (см. стр. 518), 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 смонтируйте 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 также можно загружать обновления из локальной или сетевой папки. Можно 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.

Можно 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 нужно 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 приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.
2. Нажмите на **Загрузка обновлений в хранилище Сервера администрирования**.
3. Перейдите на вкладку **Параметры приложения**.
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.

Теперь обновления загружаются в хранилище Сервера администрирования из указанных источников.

Одобрение и отклонение обновлений программного обеспечения

Параметры задачи установки обновлений могут требовать одобрения обновлений, которые должны быть установлены. Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

Например, вы можете сначала проверить установку обновлений в тестовом окружении и убедиться, что они не мешают работе устройств, и только потом установить эти обновления на клиентские устройства.

Одобрение и отклонение обновлений доступно только для Агента администрирования и управляемых приложений, установленных на клиентских устройствах под управлением Windows. Бесшовное обновление Сервера администрирования, Kaspersky Security Center Web Console и веб-плагинов управления не поддерживается. Для обновления этих компонентов вам необходимо скачать их последние версии с сайта "Лаборатории Касперского" https://www.kaspersky.ru/small-to-medium-business-security.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

   Для обновлений управляемых приложений может потребоваться установка определенной минимальной версии Kaspersky Security Center. Если эта версия более поздняя, чем ваша текущая, эти обновления отображаются, но не могут быть одобрены. Также из таких обновлений невозможно создать инсталляционные пакеты, пока вы не обновите Kaspersky Security Center. Вам будет предложено обновить ваш экземпляр Kaspersky Security Center до необходимой минимальной версии.

2. При необходимости примите Лицензионное соглашение, нажав на кнопку **Просмотреть и принять Лицензионные соглашения**.
3. Выберите обновления, которые требуется подтвердить или отклонить.
4. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или на кнопку **Отклонить**, чтобы отклонить выбранное обновление.

   По умолчанию установлено значение *Не определено*.

Обновления, для которых вы установили статус *Одобрено*, помещаются в очередь на установку.

Обновления, для которых вы установили статус *Отклонено*, деинсталлируются (если это возможно) с устройств, на которые они были ранее установлены. Также они не будут установлены на устройства позже.

Некоторые обновления для приложений "Лаборатории Касперского" невозможно деинсталлировать. Если вы установили для них статус *Отклонено*, Kaspersky Security Center не будет деинсталлировать эти обновления с устройств, на которые они были установлены ранее. Такие обновления никогда не будут установлены на устройства в будущем.
Если вы устанавливаете статус *Отклонено* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. Если вам потребуется удалить обновления, вы можете сделать это вручную локально.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....515

kaspersky

Автоматическая установка обновлений для Kaspersky Endpoint Security для Windows

Вы можете настроить автоматическое обновление баз и модулей приложения Kaspersky Endpoint Security для Windows на клиентских устройствах.

► *Чтобы настроить загрузку и автоматическую установку обновлений Kaspersky Endpoint Security для Windows на устройства:*

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

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для приложения Kaspersky Endpoint Security для Windows выберите подтип задачи **Обновление**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите область действия задачи.
6. Укажите группу администрирования, выборку устройств или устройства, к которым применяется задача.
7. Если вы включите параметр **Открыть задачу после создания** на странице **Завершение создания задачи**, вы сможете изменить установленные по умолчанию значения параметров задачи. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
8. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
9. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
10. В окне свойств задачи обновления на вкладке **Параметры приложения** укажите локальный или мобильный режим:
    - **Локальный режим**: между устройством и Сервером администрирования установлена связь.
    - **Мобильный режим**: между устройством и Kaspersky Security Center не установлена связь (например, если устройство не подключено к интернету).
11. Включите источники обновлений, которые вы хотите использовать для обновления баз и модулей приложения для Kaspersky Endpoint Security для Windows. Если требуется изменить положение источников обновлений в списке, используйте кнопки **Вверх** и **Вниз**. Если включено несколько источников обновлений, Kaspersky Endpoint Security для Windows пытается подключиться к ним один за другим, начиная с верхней части списка, и выполняет задачу обновления, извлекая пакет обновления из первого доступного источника.
12. Включите параметр **Устанавливать одобренные обновления модулей приложений**, чтобы загружать и устанавливать обновления модулей приложений вместе с базами приложений.

    Если параметр включен, то Kaspersky Endpoint Security для Windows уведомляет пользователя о доступных обновлениях модулей приложения и во время выполнения задачи обновления включает обновления модулей приложения в пакет обновлений. Kaspersky Endpoint Security для Windows устанавливает только те обновления, для которых вы установили статус *Одобрено*; обновления будут установлены локально через интерфейс приложения или через Kaspersky Security Center.

Вы также можете включить параметр **Автоматически устанавливать критические обновления модуля приложения**. При наличии обновлений модулей приложения Kaspersky Endpoint Security для Windows устанавливает обновления со статусом *Предельный* автоматически; остальные обновления модулей приложения – после одобрения их установки администратором.

Если обновление модулей приложения предполагает ознакомление и согласие с положениями Лицензионного соглашения и Политики конфиденциальности, то приложение устанавливает обновление после согласия пользователя с положениями Лицензионного соглашения и Политики конфиденциальности.

13. Установите флажок **Копировать обновления в папку**, чтобы приложение сохраняло загруженные обновления в папку, а затем укажите путь к папке.
14. Задайте расписание запуска задачи. Чтобы обеспечить своевременное обновление, рекомендуется выбрать вариант **При загрузке обновлений в хранилище**.
15. Нажмите на кнопку **Сохранить**.

При выполнении задачи **Обновление** приложение отправляет запросы серверам обновлений "Лаборатории Касперского".

Некоторые обновления требуют установки последних версий плагинов управляемых приложений.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского".....515

Об использовании файлов различий для обновления баз и модулей приложений "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 модулями приложения. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и модулей приложений. 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 модулей приложений.

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 приложений "Лаборатории Касперского" 515

Включение функции загрузки файлов различий: сценарий 540

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. 524).

pp. Включение функции для точки распространения

Включить функцию для точки распространения, которая получает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения* (см. стр. 530).

Включите функцию в параметрах политики Агента администрирования для точки распространения, которая получает обновления с Сервера администрирования (см. стр. 425).

Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

Эта функция включается в свойствах политики Агента администрирования (см. стр. 425) и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения** (см. стр. 541).

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 модулей приложений "Лаборатории Касперского" 53

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" 515

Об обновлении баз, модулей приложений и приложений "Лаборатории Касперского" 518

kaspersky

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 вкладке **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. 539).

По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" 515

Обновление баз и модулей приложений "Лаборатории Касперского" на автономных устройствах

Установка обновлений исполняемых модулей приложений "Лаборатории Касперского", не прошедших сертификационные испытания в установленном порядке (кроме обновлений, устраняющих известные уязвимости), ведет к выходу приложения из сертифицированного состояния.

Обновление баз и модулей приложений "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление (см. стр. 515) с помощью хранилища Сервера администрирования.

Когда вам необходимо обновить базы данных и модули приложений 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 приложения безопасности, установленного на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должно быть установлено это приложение 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 установлено такое же приложение 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 модулей приложений путем копирования их из хранилища Сервера администрирования.

► *Чтобы обновить базы данных и модули приложений "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:

   - Справка Kaspersky Endpoint Security для Linux
   - 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 модули приложений "Лаборатории Касперского" будут обновлены на устройстве.

См. также:

Сценарий: регулярное обновление баз и приложений "Лаборатории Касперского" 515
Создание задачи Загрузка обновлений в хранилище Сервера администрирования 524

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 приложения 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 приложения 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.

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. 607), 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.

2. 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. 608).

3. Выполнение рекомендуемых действий для критических и предупреждающих уведомлений

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации (см. стр. 600).

4. Просмотр состояния безопасности сети вашей организации

   Инструкции:

   - Просмотр веб-виджета Состояние защиты (см. стр. 551).
   - Генерация и просмотр отчета о состоянии защиты (см. стр. 561).
   - Генерация и просмотр отчета об ошибках (см. стр. 561).

5. Нахождение незащищенных клиентских устройств

   Инструкции:

   - Просмотр веб-виджета Новые устройства (см. стр. 551)
   - Генерация и просмотр отчета о развертывании защиты (см. стр. 561).

6. Проверка защиты клиентских устройств

   Инструкции:

   - Генерация и просмотр отчета из категорий Статус защиты и Статистика угроз (см. стр. 561).
   - Запуск и просмотр выборки событий Критические (см. стр. 591).

7. Оценка и ограничение загрузки событий в базу данных

   Информация о событиях, которые возникают во время работы управляемых приложений, 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. 188).

8. Просмотр информации о лицензии

   Инструкции:

   - Добавление веб-виджета Используемые лицензионные ключи на панель мониторинга и его просмотр (см. стр. 551).
   - Генерация и просмотр отчета Отчет об использовании лицензионных ключей (см. стр. 561).

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 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.

Срабатывание правил в режиме Интеллектуального обучения

В этом разделе представлена информация об обнаружениях, выполненных правилами Адаптивного контроля аномалий Kaspersky Endpoint Security для Windows на клиентских устройствах.

Правила обнаруживают аномальное поведение на клиентских устройствах и могут блокировать его. Если правила работают в режиме Интеллектуального обучения, они обнаруживают аномальное поведение и отправляют отчеты о каждом таком случае на Сервер администрирования. Эта информация хранится в виде списка в папке **Срабатывание правил в статусе Интеллектуальное обучение**, вложенной в папку **Хранилища**. Вы можете подтвердить обнаружение как корректное (см. стр. 547) или добавить его в исключения (см. стр. 549), после чего такой тип поведения не будет считаться аномальным.

Информация об обнаружениях хранится в журнале событий (см. стр. 589) на Сервере администрирования (вместе с остальными событиями) и в отчете Адаптивный контроль аномалий (см. стр. 556).

Подробная информация об Адаптивном контроле аномалий, его правилах, их режимах и статусах приведена в справке Kaspersky Endpoint Security для Windows.

В этом разделе

Просмотр списка обнаружений, выполненных с помощью правил Адаптивного контроля аномалий

► *Чтобы просмотреть список обнаружений, выполненных с помощью правил Адаптивного контроля аномалий:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).

   В списке отображается следующая информация об обнаружении, выполняемая с помощью правил Адаптивного контроля аномалий:

   - **Группа администрирования**

     Имя группы администрирования, в которую включено устройство.

   - **Имя устройства**

     Имя клиентского устройства, на котором было применено правило.

   - **Имя**

     Имя правила, которое было применено.

   - **Состояние**

     Исключение – если администратор обработал это обнаружение и добавил его как исключение из правил. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

     Подтверждение – если администратор обработал это обнаружение и подтвердил его. Этот статус остается до тех пор, пока не будет выполнена синхронизация клиентского устройства с Сервером администрирования; после синхронизации обнаружение пропадет из списка.

Пусто – если администратор не обработал обнаружение.

- **Количество срабатываний для всех правил**

  Количество обнаружений одного эвристического правила, одного процесса и одного клиентского устройства. Это количество рассчитано Kaspersky Endpoint Security.

- **Имя пользователя**

  Имя пользователя клиентского устройства, запустившего процесс, который сгенерировал обнаружение.

- **Путь исходного объекта**

  Путь к исходному процессу, то есть к процессу, выполнившему действие (подобную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного процесса**

  Хеш SHA256 исходного файла процесса (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь исходного объекта**

  Путь к объекту, который запустил процесс (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш исходного объекта**

  Хеш SHA256 исходного файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого процесса**

  Путь к целевому процессу (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого процесса**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Путь целевого объекта**

  Путь к целевому объекту (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Хеш целевого объекта**

  Хеш SHA256 целевого файла (подробную информацию см. в справке Kaspersky Endpoint Security).

- **Обработано**

  Дата обнаружения аномалии.

► *Чтобы просмотреть свойства каждого элемента:*

1. В дереве консоли выберите требуемый узел Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области папки **Срабатывание правил в статусе Интеллектуальное обучение** выберите нужный объект.

4. Выполните одно из следующих действий:
   - Перейдите по ссылке **Свойства** в рабочей области в правой части экрана.
   - В контекстном меню объекта выберите пункт **Свойства**.

   В открывшемся окне свойства объекта отображается информация объекта.

Вы можете подтвердить или добавить в исключения любой объект в списке, обнаруженный правилами Адаптивного контроля аномалий (см. стр. 546).

► *Чтобы подтвердить объект,*

выберите один или несколько элементов в списке обнаружений и нажмите на кнопку **Подтвердить**.

Статус элементов будет изменен на **Подтверждение**.

Ваше подтверждение влияет на статистику, используемую правилами (подробную информацию см. в справке Kaspersky Endpoint Security 11 для Windows).

► *Чтобы добавить объект в исключения,*

В контекстном меню объекта (или нескольких объектов) списка обнаружений выберите пункт **Добавить в исключения**.

В результате запустится мастер добавления исключений (см. стр. 549). Следуйте инструкциям мастера.

Если вы отклоните или подтвердите объект, он будет исключен из списка обнаружений после следующей синхронизации клиентского устройства с Сервером администрирования и больше не будет отображаться в списке.

Добавление исключений в правила Адаптивного контроля аномалий

Мастер добавления исключений позволяет добавлять исключения из правил Адаптивного контроля аномалий для Kaspersky Endpoint Security.

Вы можете запустить мастер с помощью одного из способов ниже.

► *Чтобы запустить мастер добавления исключений в папке Адаптивный контроль аномалий:*

1. В дереве консоли выберите узел с именем нужного вам Сервера администрирования.
2. Выберите подпапку **Срабатывание правил в статусе Интеллектуальное обучение** (по умолчанию она находится в папке **Дополнительно** → **Хранилища**).
3. В рабочей области в списке обнаружений в контекстном меню объекта (или нескольких объектов) выберите пункт **Добавить в исключения**.

   За один раз можно добавить до 1000 исключений. Если вы выберете больше элементов и попытаетесь добавить их в исключения, появится сообщение об ошибке.

   В результате запустится мастер добавления исключений. Для продолжения работы мастера нажмите на кнопку **Далее**.

Чтобы запустить мастер добавления исключений из других узлов в дереве консоли:

- Откройте вкладку **События** главного окна Сервера администрирования, затем выберите **Запросы пользователей** или **Последние события**.
- В окне **Отчет о состоянии правил Адаптивного контроля аномалий** выберите столбец **Количество обнаружений.**

► *Чтобы добавить исключения из правил Адаптивного контроля аномалий с помощью мастера добавления исключений:*

1. На первом шаге мастера выберите приложение из списка приложение "Лаборатории Касперского", чьи плагины управления позволяют добавлять исключения в политики для этих приложений.

   Этот шаг можно пропустить, если у вас есть только приложения Kaspersky Endpoint Security для Windows и нет других приложений, поддерживающих правила Адаптивного контроля аномалий.

2. Выберите политики и профили политик, в которые вы хотите добавить исключения.

   Следующий шаг отображает ход обработки политики. Вы можете прервать обработку политики, нажав на кнопку **Отмена**.

   Унаследованные политики не могут быть обновлены. Если у вас нет прав на изменение политики, такая политика также не будет обновлена.

   Когда все политики обработаны (или обработка политик прервана), создается отчет. Отчет отображает, какие политики были успешно обновлены (зеленый значок), а какие политики не были обновлены (красный значок).

3. Нажмите на кнопку **Готово**, чтобы завершить работу мастера.

   Исключение из правил Адаптивного контроля аномалий настроено и применено.

Панель мониторинга и веб-виджеты

В этом разделе содержится информация о панели мониторинга и веб-виджетах, представленных в панели мониторинга. Раздел содержит инструкции по управлению веб-виджетами и настройке веб-виджетов.

В этом разделе

kaspersky

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**.

В 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.**
- **Обновление.**
- **Статистика угроз.**
- **Другие.**

Некоторые веб-виджеты имеют текст со ссылками. Чтобы просмотреть подробную информацию, перейдите по ссылке.

При настройке панели мониторинга можно добавлять необходимые веб-виджеты (см. стр. 551), скрывать веб-виджеты (см. стр. 552), а также менять внешний вид или размер веб-виджетов (см. стр. 553), перемещать веб-виджеты (см. стр. 552) и изменять параметры веб-виджетов (см. стр. 553).

См. также:

Сценарий: мониторинг и отчеты.....544

Добавление веб-виджета на информационную панель

► *Чтобы добавить веб-виджет на информационную панель:*

1. В главном окне приложения 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. 553) и параметры (см. стр. 553) добавленных веб-виджетов.

См. также:

Сценарий: мониторинг и отчеты 544

Удаление веб-виджета с информационной панели

► *Чтобы удалить веб-виджет с информационной панели:*

1. В главном окне приложения 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. 551).

См. также:

Сценарий: мониторинг и отчеты 544

Перемещение веб-виджета на информационной панели

► *Чтобы переместить веб-виджет на информационной панели:*

1. В главном окне приложения 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 544

kaspersky

Изменение размера или внешнего вида веб-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 приложения 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 (только столбчатая диаграмма).**
     - **Максимальный.**

Внешний вид выбранного веб-виджета будет изменен.

См. также:

Сценарий: мониторинг и отчеты 544

Изменение параметров веб-виджета

► *Чтобы изменить параметры веб-виджета:*

1. В главном окне приложения 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.

После изменения параметров веб-виджета вы можете обновить данные веб-виджета вручную.

► *Чтобы обновить данные веб-виджета:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
2. Нажмите на значок параметров () рядом с веб-виджетом, который требуется переместить.
3. Нажмите на кнопку **Обновить**.

Данные веб-виджета обновлены.

См. также:

Сценарий: мониторинг и отчеты 544

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга (см. стр. 555) 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 в 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. 478) в функциональной области **Общие функции: Права пользователя**.

См. также:

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга (см. стр. 554) убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Изменения списков управления доступом к объектам** (см. стр. 478) в функциональной области **Общие функции: Права пользователей**. Если у вас нет этого права, вкладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** (см. стр. 478) 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 невозможно.

► *Чтобы настроить режим Просмотра только панели мониторинга:*

1. В главном окне приложения 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 вкладку **Панель мониторинга**.

   На открывшейся вкладке 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 невозможно изменить панель мониторинга. После выключения параметра можно управлять веб-виджетами.
5. Настройте внешний вид панели мониторинга. Набор веб-виджетов, подготовленный на вкладке **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. 551) на панель мониторинга.
   - Скрывать веб-виджеты (см. стр. 552), которые не нужны пользователю.
   - Перемещать веб-виджеты (см. стр. 552) в определенном порядке.

- Изменять размер или внешний вид (см. стр. 553) веб-виджетов.
- Изменение параметров веб-виджетов (см. стр. 553).

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 приложений "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права (см. стр. 478) для этого пользователя. После этого данные приложений "Лаборатории Касперского" отображаются у пользователя в веб-виджетах этих приложений.

Теперь пользователь может входить в Kaspersky Security Center под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

В этом разделе

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Kaspersky Security Center 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.**
- **Обновление.**
- **Статистика угроз.**
- **Другие.**

Вы можете создавать пользовательские шаблоны отчетов (см. стр. 557), редактировать шаблоны отчетов (см. стр. 558) и удалять их (см. стр. 565).

Можно создавать отчеты (см. стр. 561) на основе существующих шаблонов, экспортировать отчеты в файл (см. стр. 561) и создавать задачи рассылки отчетов (см. стр. 562).

См. также:

Сценарий: мониторинг и отчеты.....544

Создание шаблона отчета

► *Чтобы создать шаблон отчета:*

1. В главном окне приложения 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. Введите название отчета и выберите тип отчета.
4. На шаге **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 шаге **Период отчета** укажите период, за который будет формироваться отчет. Доступные значения:
   - между двумя указанными датами;
   - от указанной даты до даты создания отчета;
   - от даты создания отчета минус указанное количество дней до даты создания отчета.

   В некоторых отчетах эта страница может не отображаться.
6. Нажмите на кнопку **ОК**, чтобы завершить работу мастера.
7. Выполните одно из следующих действий:
   - Нажмите на кнопку **Сохранить и запустить**, чтобы сохранить новый шаблон отчета и запустить формирование отчета на его основе.

     Шаблон отчета будет сохранен. Отчет будет сформирован.

- Нажмите на кнопку **Сохранить**, чтобы сохранить новый шаблон отчета.

  Шаблон отчета будет сохранен.

Созданный шаблон можно использовать для формирования и просмотра отчетов.

См. также:

Сценарий: мониторинг и отчеты.....544

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 приложения 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. 561), 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:
   - Вкладка **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. 561).

       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 Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Data wait interval (min)**

  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 **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 этого параметра 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 через заданные интервалы времени (указанные в часах) 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.

- Вкладка **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.

kaspersky

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 приложения 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.

     Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите 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 приложения 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 вкладке **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 вкладке **Подробнее** отобразится таблица с подробными данными отчета.

См. также:

Сценарий: обновление приложений сторонних производителей 673
Сценарий: мониторинг и отчеты....544

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

► *Чтобы создать задачу рассылки отчета:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Новая задача рассылки отчетов**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На шаге мастера **Параметры новой задачи** введите название задачи.

   Название задачи по умолчанию – **Рассылка отчетов.** Если задача с таким названием уже существует, к названию задачи добавляется порядковый номер (<N>).
5. На шаге мастера **Конфигурация отчета** укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей.
   b. Формат отчета: HTML, XLS или PDF.

      Инструмент wkhtmltopdf необходим для преобразования отчета в формат PDF. При выборе параметра PDF Сервер администрирования проверяет, установлена ли на устройстве утилита wkhtmltopdf. Если инструмент не установлен, приложение выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.

c. Будут ли отчеты рассылаться по электронной почте, а также параметры почтовых уведомлений.

   Вы можете указать до 20 адресов электронной почты. Чтобы разделить адреса электронной почты, нажмите на клавишу **Enter**. Вы также можете вставить список адресов электронной почты, разделенных запятыми, и нажать на клавишу **Enter**.

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).

6. На шаге мастера **Настройка расписания задачи** выберите период запуска задачи.

   Доступны следующие варианты расписания запуска задачи:

- **Вручную**

Задача не запускается автоматически. Вы можете запустить задачу только вручную.

По умолчанию выбран этот вариант.

- **Каждые 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 6 часов, начиная с текущих системной даты и времени.

- **Каждые N дней**

  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 приложением, для которого 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 каждую пятницу в текущее системное время.

- **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.

- **В указанные дни**
- **При обнаружении вирусной атаки**

Запускать задачу после возникновения события *Вирусная атака*. Выберите типы приложений, которые будут отслеживать вирусные атаки. Доступны следующие типы приложений:

- антивирусы для рабочих станций и файловых серверов;
- антивирусы защиты периметра;
- антивирусы для почтовых систем.

По умолчанию выбраны все типы приложений.

Вы можете запускать разные задачи в зависимости от типа приложения безопасности, сообщающего о вирусной атаке. В этом случае удалите выбор типов приложений, которые вам не нужны.

- **По завершении другой задачи**

Текущая задача будет запущена после завершения другой задачи. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам. Например, вы можете запустить задачу *Управление устройствами* с помощью параметра **Включить устройство** и после ее завершения запустить задачу *Поиск вирусов*, как запускающую задачу.

Вам нужно выбрать запускающую задачу из таблицы и статус, с которым эта задача должна завершиться (**Завершена успешно** или **Сбой**).

При необходимости вы можете искать, сортировать и фильтровать задачи в таблице следующим образом:

- Введите название задачи в поле поиска, чтобы выполнить поиск задачи по названию.
- Нажмите на значок сортировки, чтобы отсортировать задачи по имени.

  По умолчанию задачи отсортированы в алфавитном порядке по возрастанию.
- Нажмите на значок фильтра и в открывшемся окне отфильтруйте задачи по группам, после чего нажмите на кнопку **Применить**.

1. На этом шаге мастера настройте другие параметры расписания запуска задачи:
   - В разделе **Расписание задачи** проверьте или перенастройте ранее выбранное расписание и установите период, дни месяца или недели, задайте условие вирусной атаки или выполнение другой задачи в качестве запуска задачи. В этом разделе также можно указать время запуска, если выбрано подходящее расписание.
   - В разделе **Дополнительные параметры** укажите следующие параметры:
     - **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 приложения "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. Для расписания **Вручную**, **Один раз** и **Немедленно** задачи выполняются только на тех клиентских устройствах, которые видны в сети. Например, вы можете выключить этот параметр для ресурсоемкой задачи, которую вы хотите запустить только вне рабочих часов.

       По умолчанию параметр выключен.

- **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 автоматическую случайную задержку запуска задачи в интервале**

  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**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

2. На шаге мастера **Выбор учетной записи для запуска задачи** укажите учетные данные учетной записи, которая используется для запуска задачи.
3. Если требуется изменить другие параметры задачи после ее создания, на шаге мастера **Завершение создания задачи** включите параметр **Открыть окно свойств задачи после ее создания**. По умолчанию параметр включен.
4. Нажмите на кнопку **Готово**, 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 приложения 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 544

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

kaspersky

О событиях в Kaspersky Security Center

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "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 приложениях "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 приложений "Лаборатории Касперского". Каждое управляемое приложение "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать приложение, можно на вкладке **Настройка событий** в свойствах политики приложения. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими приложениями:

- Компоненты приложения Kaspersky Security Center:
  - Сервер администрирования (см. стр. 569)
  - Агент администрирования (см. стр. 586)
- Управляемые приложения "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми приложениями "Лаборатории Касперского", см. в документации соответствующего приложения.

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 приложения 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 приложения может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе приложения или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center. Некоторые события не сохраняются в базе данных Сервера администрирования по умолчанию, поскольку для них установленное время хранения равно нулю. Во внешние системы можно экспортировать только те события, которые хранятся в базе данных Сервера администрирования не менее одного дня.

kaspersky

См. также:

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 приложениях "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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. 608).

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. 595).

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

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 приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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. 608).

Таблица 44. 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 приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц (на стр. 369), 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. 386) 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. 300) 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
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. 368). 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 невозможно 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. 370). Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ (см. стр. 369) добавлен на Сервер администрирования. • Если вы используете подписку (см. стр. 377), продлите ее. Неограниченная подписка продлевается автоматически, если предоплата поставщику услуг была своевременно внесена.	180 дней
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.	180 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Аудит: Не удалось выполнить экспорт в SIEM-систему	5130	KLAUD_EV_SIEM_EXPORT_ERROR	События этого типа возникают при сбое экспорта событий в SIEM-систему из-за ошибки соединения с SIEM-системой.	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 приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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. 608).

Таблица 45. 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений 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 приложений сторонних производителей и если количество установок превысило заданное в лицензионном ключе приложения стороннего производителя ограничение. Вы можете ответить на событие следующими способами: • Просмотрите список управляемых устройств. Удалите приложение стороннего производителя с устройств, на которых оно не используется. • Используйте лицензию стороннего производителя на большее количество устройств. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений. В группу лицензионных приложений входят приложения 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 модулей приложений.	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
Общая папка недоступна	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	События этого типа возникают, если общая папка Сервера администрирования недоступна (стр. 139). 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
Недостаточно места в базе данных 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: • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 188). • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль приложений. Вы можете изменить параметры политики Kaspersky Endpoint Security, касающиеся хранения событий компонента Контроль приложений в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД (см. стр. 229).	180 дней

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 приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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. 608).

Таблица 46. 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. 596).	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center проверяет, не превышены ли лицензионные ограничения. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения приложений "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц (см. стр. 369) 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. 386) при превышении лицензионного ограничения.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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. 331). • Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Kaspersky Security Center Web Console (см. стр. 331).	90 дней
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания приложений 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. 244).	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. 300) при выполнении которых, статус устройства изменяется на *Предупреждение*.	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
Для одной из групп лицензионных приложений скоро будет превышено ограничение числа установок	4127	KLSRV_INVLICPROD_FILLED	События этого типа возникают, если количество установок приложений сторонних производителей, включенных в группу лицензионных приложений, достигает 90% от максимально допустимого значения, указанного в свойствах лицензионного ключа. Вы можете ответить на событие следующими способами: • Если приложение стороннего производителя не используется на каких-то управляемых устройствах, удалите приложение с этих устройств. • Если вы ожидаете, что количество установок для приложения стороннего производителя превысит разрешенное ограничение в ближайшем будущем, рассмотрите возможность получения лицензии приложения стороннего производителя на большее количество устройств заранее. Вы можете управлять лицензионными ключами приложений сторонних производителей, используя функциональность групп лицензионных приложений.	90 дней
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 действия по реагированию 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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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
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

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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 действия по реагированию 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
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 жестком 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. • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования (на стр. 188). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 595). Просмотрите информацию о выборе СУБД (см. стр. 229).	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 операционной системы на устройстве, на котором установлен подчиненный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Разорвано соединение с главным Сервером администрирования	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	События этого типа возникают при разрыве соединения с главным Сервером администрирования. Прочтите журнал событий операционной системы на устройстве, на котором установлен главный Сервер администрирования, и отреагируйте соответствующим образом.	90 дней
Зарегистрированы новые обновления модулей приложений "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления приложений "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console (см. стр. 536).	90 дней

Отображаемое имя типа события	Идентификатор типа события	Тип события	Описание	Срок хранения по умолчанию
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. 598). Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования (на стр. 188). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 595).	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. 598). Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования (см. стр. 188). • Сократите список событий для хранения в базе данных Сервера администрирования (на стр. 595).	Не хранится
Аудит: Не удалось выполнить проверку подключения к SIEM-серверу	5120	KLAUD_EV_SIEM_TEST_FAILED	События этого типа возникают при сбое автоматической проверки подключения к SIEM-серверу.	90 дней

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 приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. 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. 608).

Таблица 47. 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	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Для одной из групп лицензионных приложений 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	
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_SERVER CONNECT	30 дней	

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию	Комментарий
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • группах администрирования; • группах безопасности; • пользователях; • инсталляционных пакетах; • задачах; • политиках; • 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: Свойства объекта были изменены	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 дней	Это событие отслеживает изменения в следующих параметрах: • пользователь; • лицензия; • Сервер; • виртуальный Сервер.
Аудит: Права пользователя были изменены	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	
Аудит: Проверка подключения к SIEM-серверу завершена успешно	5110	KLAUD_EV_SIEM_TEST_SUCCESS	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 с уровнем важности **Предупреждение**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования (см. стр. 608).

Таблица 48. 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

См. также:

Информационные события Агента администрирования 587

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования с уровнем важности **Информационное событие**.

Для каждого события, которое может генерировать приложение, можно указать параметры уведомлений и параметры хранения на вкладке **Настройка событий** в свойствах политики приложения. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования (см. стр. 608).

Таблица 49. Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлено приложение	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Удалено приложение	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлено наблюдаемое приложение	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалено наблюдаемое приложение	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

См. также:

События предупреждения Агента администрирования 586

kaspersky

Использование выборок событий

Выборки событий предназначены для просмотра на экране именованных наборов событий, которые выбраны из базы данных Сервера администрирования. Эти типы событий сгруппированы по следующим категориям:

- Уровень важности: **Критические события**, **Сбой**, **Предупреждение** и **Информационные события.**
- Время: **Последние события.**
- Тип: **Запросы пользователей** и **События аудита.**

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 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 приложений).
- **Последние события** (за последнюю неделю).
- **События аудита** (см. стр. 583).

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий (см. стр. 590). 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 приложения 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. 590).
- Сгенерируйте выборку событий (см. стр. 591).
- Просмотрите сведения о выбранных выборках событий (см. стр. 592).
- Удалите выборку событий (см. стр. 594).
- Удалять события из базы данных Сервера администрирования (см. стр. 594).

См. также:

Выборки устройств 304

Создание выборки событий

► *Чтобы создать выборку событий:*

1. В главном окне приложения 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 544

Изменение выборки событий

► *Чтобы изменить выборку событий:*

1. В главном окне приложения 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 вкладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно изменять все свойства.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

См. также:

Сценарий: мониторинг и отчеты 544

Просмотр списка выборки событий

► *Просмотр выборки событий:*

1. В главном окне приложения 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 544

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. 592).

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 приложения 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. 591).

► *Чтобы импортировать выборку событий:*

1. В главном окне приложения 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. 591).
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 544

Экспорт событий в файл

► *Чтобы экспортировать события в файл:*

1. Запустите выборку событий (см. стр. 591).
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 544

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями (см. стр. 634), вы можете перейти к истории ревизий объекта.

► *Чтобы просмотреть историю объекта из события:*

1. Запустите выборку событий (см. стр. 591).
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

См. также:

Сценарий: мониторинг и отчеты 544

Удаление событий

► *Чтобы удалить одно или несколько событий:*

1. Запустите выборку событий (см. стр. 591).
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 544

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий невозможно удалить.

► *Чтобы удалить выборки событий:*

1. В главном окне приложения 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 544

kaspersky

Настройка срока хранения события

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и приложений "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 приложения "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 приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выполните одно из следующих действий:
   - Чтобы настроить срок хранения событий Агента администрирования или управляемого приложения "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 вкладку **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

О блокировке частых событий

Управляемое приложение, например Kaspersky Endpoint Security для Linux, установленное 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. 188).

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. 597) получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать (на стр. 597) 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. 597) 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 вкладке **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 вкладке **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 приложения 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, приложение 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, приложение вычисляет приблизительный размер дискового пространства для хранения указанного числа событий. Вы можете использовать этот расчет, чтобы оценить, достаточно ли у вас свободного дискового пространства, чтобы избежать переполнения базы данных. По умолчанию емкость базы данных Сервера администрирования – 400 000 событий. Максимальная рекомендованная емкость базы данных – 45 000 000 событий.

Приложение проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, приложение 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 операционной системы. 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.

kaspersky

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. 600) 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. 608).

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 приложения перейдите в раздел **Мониторинг и отчеты** → **Уведомления**.

   На левой панели выбрана категория **Все уведомлени**я, 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 приложениях "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 приложений "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 приложение безопасности на устройства, просмотреть список устройств или список событий (см. стр. 336). 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 вкладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите вкладку **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 вкладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на вкладке **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. 551).

   Веб-виджет отображается на вкладке **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. 553), 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 50. Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Не установлено приложение безопасности	Агент администрирования установлен на устройстве, но не установлено приложение 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.
Давно не выполнялся поиск вредоносного ПО	Устройство видимо в сети и на устройстве установлено приложение 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 установлено приложение 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.

Условие	Описание условия	Доступные значения
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 приложение требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые приложения	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые приложения.	• Переключатель выключен. • Переключатель включен.
Обнаружены уязвимости в приложениях	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 приложениях с заданным уровнем критичности.	• Предельный. • Высокий. • Средний. • Игнорировать, если невозможно закрыть уязвимость. • Игнорировать, если обновление назначено к установке.
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
Давно не выполнялась проверка обновлений Центра обновления Windows	Не выполнялась задача *Синхронизация обновлений Windows Update* больше указанного времени.	Более 1 дня.
Недопустимый статус шифрования	Агент администрирования установлен на устройстве, но результат шифрования устройства равен указанному значению.	• Не соответствует политике из-за отказа пользователя (только для внешних устройств). • Не соответствует политике из-за ошибки. • В процессе применения политики – требуется перезагрузка. • Не задана политика шифрования. • Не поддерживается. • В процессе применения политики.
Параметры мобильного устройства не соответствуют политике	Параметры мобильного устройства отличаются от параметров, заданных в политике Kaspersky Endpoint Security для Android при выполнении проверки правил соответствия.	• Переключатель выключен. • Переключатель включен.
Есть необработанные проблемы безопасности	На устройстве есть необработанные проблемы безопасности. Проблемы безопасности могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых приложений "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен приложением	Статус устройства определяется управляемым приложением.	• Переключатель выключен. • Переключатель включен.

Условие	Описание условия	Доступные значения
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *ОК*, когда устройство успешно синхронизировано с Сервером администрирования и свободное дисковое пространство устройства больше или равно указанному значению.	Более чем 0 МБ.
Устройство стало неуправляемым	Устройство определяется видимым в сети при обнаружении устройств, но было выполнено более трех неудачных попыток синхронизации с Сервером администрирования.	• Переключатель выключен. • Переключатель включен.
Защита выключена	Устройство видимо в сети, но приложение безопасности на устройстве отключено больше указанного времени. В этом случае состояние приложения безопасности *Остановлено* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлено*.	Более чем 0 минут.
Не запущено приложение безопасности	Устройство видимо в сети и приложение безопасности установлено на устройстве, но не запущено.	• 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. столбец "Описание условий" в таблице выше) 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 607

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

► *Чтобы изменить статус устройства на* Критический*:*

1. В главном окне приложения 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 вкладку **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 приложения 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 вкладку **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 598

О статусах устройства 296

Сценарий: мониторинг и отчеты 544

Сценарий: настройка защиты сети 393

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 приложение Kaspersky Security Center посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события приложение 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 вкладку с требуемым способом уведомления:
   - **Электронная почта**

На вкладке **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 доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного центра сертификации.

- Выберите файл сертификата клиента:

  Вы можете использовать сертификат, полученный из любого источника, например, от любого доверенного центра сертификации. Вам нужно указать сертификат и его закрытый ключ, используя один из следующих типов сертификатов:

  - Сертификат X-509:

  Вам нужно 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:

  Вам нужно 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: приложение 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 вашего электронного письма. 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 приложением 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. 614).

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 приложение может отправлять за указанный интервал времени.

- **SMS**

  На вкладке **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 доверенного центра сертификации и загрузить его на Сервер администрирования. Kaspersky Security Center проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center не может подключиться к SMTP-серверу, если сертификат SMTP-сервера не получен от доверенного 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 вашего электронного письма. 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 приложением при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена (см. стр. 614).

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: приложение отправляет тестовые сообщения указанным получателям.

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

- **Исполняемый файл для запуска**

  Если выбран этот способ уведомления, в поле ввода можно указать, какое приложение будет запущено 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. 614). Указанные папка и файл должны

находиться на Сервере администрирования.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое приложение может отправлять за указанный интервал времени.

1. На вкладке 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. 411) для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах приложения.

См. также:

Сценарий: мониторинг и отчеты.....544

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 приложения 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 приложений безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR https://www.eicar.org.

kaspersky

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 51. 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
%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.

kaspersky

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

В этом разделе

Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"** предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, 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 приложения "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для приложений "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в приложениях "Лаборатории Касперского". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию (см. стр. 617).

  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. 368), которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

Рекламные объявления включают информацию о специальных предложениях для ваших приложений "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. 617).

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. 445).

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" приложение 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. 616), 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. 617).

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" (см. стр. 615) 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 приложения 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. 615) (**Мониторинг и отчеты → Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых приложениях, 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 вкладке **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.

kaspersky

Cloud Discovery

Kaspersky Security Center позволяет отслеживать использование облачных сервисов на управляемых устройствах с операционной системой Windows и блокировать доступ к нежелательным облачным сервисам. Cloud Discovery отслеживает попытки пользователей получить доступ к этим службам через браузеры и настольные приложения. Также отслеживает попытки доступа пользователей к облачным сервисам через незашифрованные соединения (например, по протоколу HTTP). Эта функция позволяет выявлять и прекращать скрытое несанкционированное использование облачных сервисов.

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center по лицензии Kaspersky Security Center EDR Optimum или XDR Expert.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Можно включить функцию Cloud Discovery (см. стр. 619) и выбрать политики безопасности или профили, для которых ее требуется включить. Можно также включать и выключать функцию отдельно для каждой политики безопасности или профиля. Вы можете заблокировать доступ к облачным сервисам (см. стр. 621), к которым вы хотите ограничить доступ для пользователей.

Чтобы заблокировать доступ к нежелательным облачным сервисам, убедитесь, что выполнены следующие условия:

- Вы используете версию Kaspersky Endpoint Security 11.2 для Windows или выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.
- Вы приобрели лицензию на Kaspersky NEXT, которая дает возможность блокировать доступ к нежелательным облачным сервисам. Подробнее см. справку Kaspersky Next. Подробную информацию см. в справке Kaspersky Next https://support.kaspersky.ru/help/NextPro/1.0/ru-ru/101540.htm. Лицензия Kaspersky NEXT недоступна на территории Республики Беларусь.

Информация об удачных и заблокированных попытках доступа к облачным сервисам отображается в веб-виджете Cloud Discovery (см. стр. 620) и в отчетах Cloud Discovery. Веб-виджет также показывает уровень риска каждого облачного сервиса. Kaspersky Security Center получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности или профилями политик, в которых она включена (см. стр. 619).

В этом разделе

kaspersky

Включение функции Cloud Discovery с помощью веб-виджета

Функция Cloud Discovery получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных политиками безопасности, в которых она включена. Включить или выключить Cloud Discovery можно только для политики Kaspersky Endpoint Security для Windows.

Существуют два способа включить функцию Cloud Discovery:

- С помощью веб-виджета Cloud Discovery.
- В свойствах политики Kaspersky Endpoint Security для Windows.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.4/ru-RU/187200.htm.

Обратите внимание, что вы можете выключить функцию Cloud Discovery только в параметрах политики Kaspersky Endpoint Security для Windows.

Чтобы включить Cloud Discovery, у вас должно быть право **Запись** в функциональной области **Общий функционал: Базовая функциональность**.

► *Чтобы включить функцию Cloud Discovery с помощью веб-виджета Cloud Discovery:*

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
3. В веб-виджете **Cloud Discovery** нажмите на кнопку **Включить**.

   Если у вас установлен Kaspersky Endpoint Security для Windows версии 12.4, включите функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows. Подробнее см. раздел Cloud Discovery справки Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.4/ru-RU/187200.htm.
   Если у вас версия Kaspersky Endpoint Security для Windows ниже версии 12.4, обновите плагин Kaspersky Endpoint Security для Windows до версии 12.5.

4. В открывшемся окне **Включить Cloud Discovery** выберите политики безопасности, для которых вы хотите включить функцию и нажмите на кнопку **Включить**.

   Следующие параметры политики будут включены автоматически: **Внедрение скрипта в веб-трафик для взаимодействия с веб-страницами**, **Мониторинг веб-сеансов** и **Проверка зашифрованных подключений**.

Функция Cloud Discovery включена, веб-виджет добавлен в панель мониторинга.

Добавление веб-виджета Cloud Discovery в панель мониторинга

Вы можете добавить веб-виджет **Cloud Discovery** в панель мониторинга, чтобы отслеживать использование облачных сервисов на управляемых устройствах.

Чтобы добавить веб-виджет Cloud Discovery в панель инструментов, у вас должно быть право **Запись** в функциональной области **Общий функционал: Базовая функциональность**.

► *Чтобы добавить веб-виджет Cloud Discovery в панель мониторинга:*

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.
3. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
4. В списке доступных веб-виджетов нажмите на значок шеврона () рядом с категорией **Другое**.
5. Выберите веб-виджет **Cloud Discovery** и нажмите на кнопку **Добавить**.

   Если функция Cloud Discovery выключена, следуйте инструкциям в разделе Включение функции Cloud Discovery с помощью веб-виджета (см. стр. 619).

Выбранный веб-виджет будет добавлен в конец панели мониторинга.

Просмотр информации об использовании облачных сервисов

Веб-виджет **Cloud Discovery** показывает информацию о попытках доступа к облачным сервисам. Веб-виджет также показывает уровень риска каждого облачного сервиса (см. стр. 621). Kaspersky Security Center получает информацию об использовании облачных сервисов от всех управляемых устройств, защищенных профилями безопасности, в которых они включены.

Перед просмотром убедитесь, что:

- Веб-виджет Cloud Discovery добавлен в панель мониторинга (см. стр. 619).
- Функция Cloud Discovery включена (см. стр. 619).
- У вас есть право **Чтение** в функциональной области **Общий функционал: Базовая функциональность**.

► *Чтобы посмотреть веб-виджет Cloud Discovery:*

1. Откройте Kaspersky Security Center.
2. В главном окне приложения перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

   Веб-виджет **Cloud Discovery** отображается в панели мониторинга.
3. В левой части веб-виджета **Cloud Discovery** выберите категорию облачных сервисов.

   В таблице в правой части веб-виджета отображается до пяти сервисов из выбранной категории, к которым пользователи чаще всего пытаются получить доступ. Учитываются как успешные, так и заблокированные попытки доступа.
4. В правой части веб-виджета выберите требуемый сервис.

   В таблице ниже отображается до десяти устройств, наиболее часто обращающихся к этому сервису.

В веб-виджете отображаются запрашиваемые данные.

В отображаемом веб-виджете можно выполнить следующие действия:

- Перейдите в раздел **Мониторинг и отчеты** → **Отчеты**, чтобы просмотреть отчеты Cloud Discovery.
- Заблокируйте или разрешите доступ к выбранному облачному сервису (см. стр. 621).

Возможность блокировки доступна только в том случае, если вы активировали Kaspersky Security Center по лицензии Kaspersky Security Center EDR Optimum или XDR Expert.
Возможность блокировки доступна только при использовании Kaspersky Endpoint Security 11.2 для Windows и выше. Более ранние версии приложения безопасности позволяют только контролировать использование облачных сервисов.

Уровень риска облачного сервиса

Cloud Discovery определяет уровень риска для каждого облачного сервиса. Уровень риска помогает определить службы, не соответствующие требованиям безопасности вашей организации. Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису (см. стр. 621).

Уровень риска является оценочным показателем и ничего не говорит о качестве облачного сервиса или о производителе. Уровень риска – это рекомендация экспертов "Лаборатории Касперского".

Уровни риска облачных сервисов отображаются в веб-виджете Cloud Discovery (см. стр. 620) и в списке всех контролируемых облачных сервисов (см. стр. 621).

Блокировка доступа к нежелательным облачным сервисам

Вы можете заблокировать доступ к облачным сервисам, к которым вы хотите ограничить доступ для пользователей. Вы также можете разрешить доступ к облачным сервисам, которые ранее были заблокированы.

Например, уровень риска можно учесть при принятии решения о блокировке доступа к определенному сервису (см. стр. 621).

Вы можете заблокировать или разрешить доступ к облачным сервисам для политики безопасности или профиля политики.

Существует два способа заблокировать доступ к нежелательным облачным сервисам:

- С помощью веб-виджета Cloud Discovery.

  В этом случае вы можете заблокировать доступ к сервисам по очереди.

- В свойствах политики Kaspersky Endpoint Security для Windows.

  В этом случае вы можете заблокировать доступ к сервисам по очереди или сразу всю категорию.

  Подробную информацию о том, как включить функцию Cloud Discovery в свойствах политики Kaspersky Endpoint Security для Windows, см. в разделе Cloud Discovery справки Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.4/ru-RU/187200.htm.

► *Чтобы заблокировать или разрешить доступ к облачному сервису с помощью веб-виджета:*

1. Откройте веб-виджет Cloud Discovery и выберите требуемый облачный сервис (см. стр. 620).
2. В панели **Топ-10 устройств, использующих эту службу** найдите политику безопасности или профиль политики, для которых вы хотите заблокировать или разрешить службу.
3. В соответствующей строке в столбце **Статус доступа в политике или профиле политики** выполните одно из следующих действий:
   - Чтобы заблокировать службу, в раскрывающемся списке выберите **Заблокировано**.
   - Чтобы разрешить службу, в раскрывающемся списке выберите **Разрешено**.
4. Нажмите на кнопку **Сохранить**.

Доступ к выбранной службе заблокирован или разрешен для политики безопасности или профиля политики.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

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. 624).
- Убедитесь, что у вас есть значения системных параметров (см. стр. 624).

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. 625).

- Выбор событий, которые вы хотите экспортировать в SIEM-систему

  Отметьте события, которые вы хотите экспортировать в SIEM-систему. Отметите общие события (см. стр. 629), которые возникают во всех управляемых приложениях "Лаборатории Касперского". Затем можно отметить события для экспорта для определенного управляемого приложения (см. стр. 627).

- Настройка экспорта событий в SIEM-систему

  Экспортировать события можно следующими способами:

  - Укажите протоколы TCP/IP, UDP или TLS over TCP (см. стр. 630).
  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center (см. стр. 631). 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. 634), если вы выбрали события, которые хотите экспортировать.

См. также:

kaspersky

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.

  ПротоколПротокол, используемый для передачи сообщений из Kaspersky Security Center в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center и настройках приемника в SIEM-системе.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 622

Об экспорте событий

Kaspersky Security Center позволяет получать информацию о событиях (см. стр. 567), произошедших в процессе работы Сервера администрирования и приложений "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 приложений в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и приложения. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться в 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.

Экспорт событий в формате Syslog

Вы можете отправлять события в формате Syslog в любую SIEM-систему. Используя формат Syslog, вы можете передавать любые события, произошедшие на Сервере администрирования и в приложениях «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. 630).

- **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.

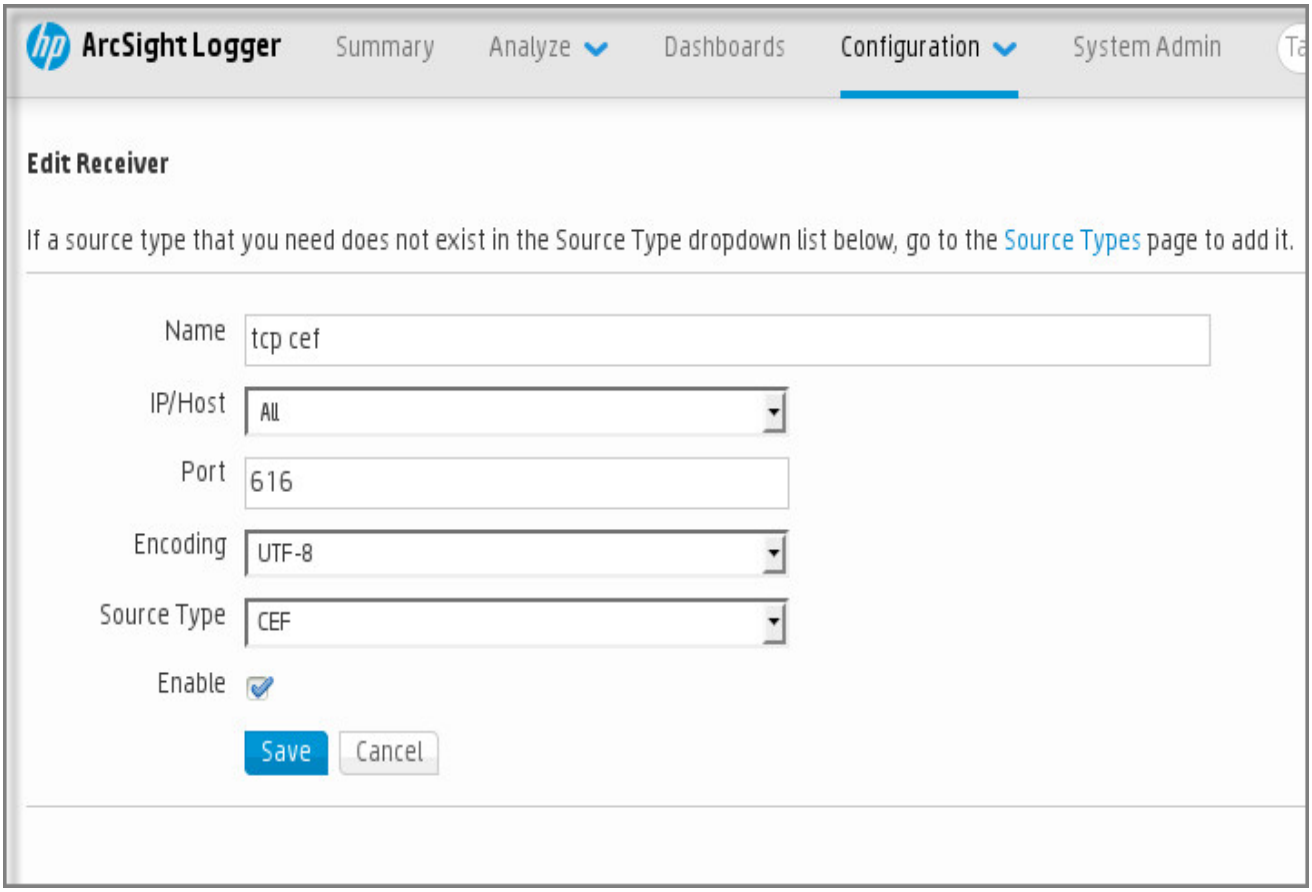


Рисунок 3. Пример настройки приемника сообщений

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.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 622

Выбор событий для экспорта в SIEM-системы в формате Syslog

В этом разделе описывается, как выбрать события для дальнейшего экспорта в SIEM-системы в формате Syslog.

kaspersky

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 622

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 приложениях, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельного приложения, управляемого этой политикой.
- Выбор событий для управляемого приложения. Если вы выбираете экспортируемые события для управляемого приложения, установленного на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этом приложении.

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 622

Выбор событий приложений "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенном управляемом приложении, установленном на управляемых устройствах, выберите события для экспорта в политике приложения. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

► *Чтобы отметить события для экспорта для определенного управляемого приложения:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Выберите политику приложения, для которого 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 управляемого приложения 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 приложения, вам не удастся переопределить выбранные события для управляемого устройства.

► *Чтобы выбрать события для управляемого устройства:*

1. В главном окне приложения 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 **Приложения**.
4. Перейдите по ссылке с названием требуемого приложения в списке приложений.
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 567

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 приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**, а затем перейдите по ссылке политики.
2. В открывшемся окне перейдите на вкладку **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 567

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других приложениях "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)используется)используется)используется)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 622

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. Заархивированные события можно экспортировать 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. Чтобы убедиться, что соединение с SIEM-системой успешно настроено, нажмите на кнопку **Проверить соединение**.

   Отобразится статус подключения.
8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует отмеченные события (см. стр. 626) в SIEM-систему. Если вы установите дату начала экспорта, Сервер администрирования также экспортирует выбранные события, хранящиеся в базе данных Сервера администрирования, с указанной даты.

См. также:

О настройке экспорта событий в SIEM-системе 625

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, приложениям, 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 приложения 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:

Сценарий: настройка экспорта событий в SIEM-системы 622

В этом разделе

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

Сценарий: настройка экспорта событий в SIEM-системы 622

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 622

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 вкладке **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 622

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.

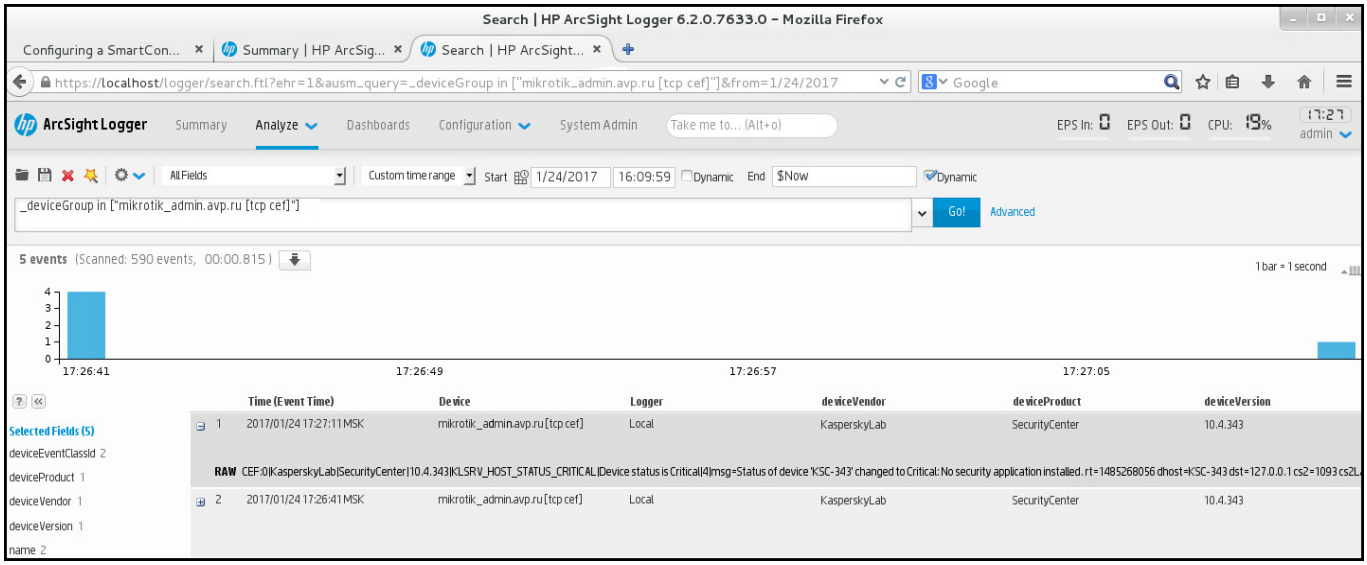


Рисунок 4. Пример событий

См. также:

Сценарий: настройка экспорта событий в SIEM-системы 622

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, которые поддерживают работу с ревизиями:

- свойства Сервера администрирования;
- политики;
- задачи;
- группы администрирования;
- учетные записи пользователей;
- инсталляционные пакеты.

Вы можете выполнять с ревизиями объектов следующие действия:

- просматривать выбранную ревизию (доступно только для политик) (см. стр. 636);
- откатывать изменения объекта к выбранной ревизии (см. стр. 636);
- сохранять ревизии в виде файла JSON (доступно только для политик) (см. стр. 636).

В окне свойств объектов, которые поддерживают работу с ревизиями, в разделе **История ревизий** отображается список ревизий объекта со следующей информацией:

- **Ревизия** – номер ревизии объекта.
- **Время** – дата и время изменения объекта.
- **Пользователь** – имя пользователя, изменившего объект.
- **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
- **IP-адрес Web Console** – IP-адрес приложения Kaspersky Security Center Web Console, с помощью которого был изменен объект.
- **Действие** – выполненное действие с объектом.
- **Описание** – описание ревизии изменения параметров объекта.

  По умолчанию описание ревизии объекта не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

См. также:

Сценарий: настройка защиты сети.....393

В этом разделе

Просмотр и сохранение ревизии политики 636

Откат изменений объекта к предыдущей ревизии 636

kaspersky

Просмотр и сохранение ревизии политики

Kaspersky Security Center позволяет просмотреть, какие изменения были внесены в политику за определенный период, и сохранить информацию об этих изменениях в файле.

Просмотр и сохранение ревизии политики доступны, если соответствующий веб-плагин управления поддерживает эту функцию.

► *Чтобы просмотреть ревизию политики:*

1. В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Политики и профили политик**.
2. Нажмите на ревизию политики, которую вы хотите просмотреть и перейдите в раздел **История ревизий**.
3. В списке ревизий политики нажмите на номер ревизии, которую вы хотите просмотреть.

   Если размер ревизии превышает 10 МБ, просмотреть ее с помощью Kaspersky Security Center Web Console невозможно. Вам будет предложено сохранить выбранную ревизию в файл JSON.

   Если размер ревизии не превышает 10 МБ, отображается отчет в формате HTML с параметрами выбранной ревизии политики. Так как отчет отображается во всплывающем окне, убедитесь, что в вашем браузере разрешены всплывающие окна.

► *Чтобы сохранить ревизию политики в файл JSON,*

В списке ревизий политики выберите ревизию, которую вы хотите сохранить и нажмите кнопку **Сохранить в файл**.

Ревизия сохранена в файле JSON.

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 вкладку **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.....393

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 безопасности;
- 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. 489) для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования приложение перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные приложения "Лаборатории Касперского" – Агент администрирования и приложение 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. 276) 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. 325). 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.
- Приложение безопасности, которое использовалось для шифрования диска, например Kaspersky Endpoint Security для Windows, установлено 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/12.3/ru-RU/130941.htm.

При удалении устройства из группы Нераспределенные устройства вручную приложение удаляет устройство из списка. После удаления устройства установленные приложения "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.

В этом разделе

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 приложения 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 приложением "Лаборатории Касперского", поместившим выбранный объект в хранилище. Приложение "Лаборатории Касперского" указано в поле **Запись добавлена**. Подробную информацию о том, какое действие необходимо выполнить, см. в документации к приложению "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 приложения;
- загрузки журналов событий;
- создание файла дампа для приложения;
- запуска диагностики и загрузки результатов диагностики;
- запуск, остановка и перезапуск приложений.

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. 648).

См. также:

Включение и выключение трассировки для приложений

Вы можете включать и выключать трассировку для приложений, включая трассировку xperf.

Включение и выключение трассировки

► *Чтобы включить или выключить трассировку на удаленном устройстве:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого 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**

Приложение 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 выбранного приложения. В некоторых случаях для включения трассировки приложения безопасности требуется перезапустить это приложение и его задачу.

> На клиентских устройствах под управлением Linux трассировка компонента Обновление Агента администрирования 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 выбранного приложения, нажмите на кнопку **Выключить трассировку**.

   Трассировка выключена для выбранного приложения.

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. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений 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 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 приложений, событиях, используемых для оценки производительности, а также события Средства оценки системы Windows.

   b. Выберите один из уровней трассировки Xperf:
      - **Базовый тип**

        Приложение получает данные трассировки во время работы приложения Kaspersky Endpoint Security.

        По умолчанию выбран этот вариант.
      - **Тип перезагрузки**

        Приложение 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 приложения

► *Чтобы загрузить файл трассировки приложения:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, для которого 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. 641).
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 приложений

► *Чтобы загрузить с клиентского устройства параметры приложений:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.
3. В разделе **Параметры приложения** нажмите на кнопку **Загрузить** для загрузки информации о параметрах приложения, 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. 641).
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 приложений.

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. 641).
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 приложения

Вы можете запускать, останавливать и перезапускать приложения на клиентском устройстве.

► *Чтобы запустить, остановить или перезапустить приложение:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В списке приложений выберите приложение, которое вы хотите запустить, остановить или перезапустить.
4. Выберите действие, нажав на одну из следующих кнопок:
   - **Остановить приложение.**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Перезапустить приложение.**

     Эта кнопка доступна, только если приложение в данный момент запущено.
   - **Запустить приложение.**

     Эта кнопка доступна, только если приложение в данный момент не запущено.

В зависимости от выбранного вами действия требуемое приложение 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 Агента администрирования Kaspersky Security Center и скачивание результатов

► *Чтобы запустить диагностику Агента администрирования Kaspersky Security Center на удаленном устройстве и загрузить ее результаты:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Приложения "Лаборатории Касперского"**.

   В разделе **Управление приложениями** откроется список приложений "Лаборатории Касперского", установленных на устройстве.
3. В разделе списке приложений выберите **Агент администрирования Kaspersky Security Center**.

   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 приложения на клиентском устройстве

Вам может потребоваться запустить приложение на клиентском устройстве, если вас об этом попросит специалист Службы технической поддержки "Лаборатории Касперского". Вам не нужно устанавливать приложение самостоятельно на этом устройстве.

► *Чтобы запустить приложение на клиентском устройстве:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Файлы приложения** нажмите на кнопку **Обзор** для выбора ZIP-архива с приложением, которое 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 указанного приложения на клиентском устройстве.
5. Следуйте указаниям сотрудника службы поддержки "Лаборатории Касперского".

Создание файла дампа для приложения

Файл дампа приложения позволяет просматривать параметры приложения, работающего на клиентском устройстве, в определенный момент времени. Этот файл также содержит информацию о модулях, которые были загружены для приложения.

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 приложения:*

1. Откройте утилиту удаленной диагностики клиентского устройства (см. стр. 641).
2. В окне удаленной диагностики выберите раздел **Запуск удаленного приложения**.
3. В разделе **Формирование дампа процесса** укажите исполняемый файл приложения, для которого вы хотите создать файл дампа.
4. Нажмите на кнопку **Загрузить**, чтобы сохранить файл дампа указанного приложения.

   Если указанное приложение не запущено 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. 640). 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 приложений, журналами событий устройства и файлом дампа для аварийных ситуаций, прерванных приложений.

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. 641). 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 приложениями сторонних производителей на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center связанные с управлением сторонних приложений на клиентских устройствах.

В этом разделе

О приложениях сторонних производителей

Kaspersky Security Center может помочь вам обновить приложения сторонних производителей, установленное на клиентских устройствах, и закрыть уязвимости приложений сторонних производителей. Kaspersky Security Center может обновлять приложения сторонних производителей только с текущей версии до последней версии. В следующем списке представлены приложения сторонних производителей, которые вы можете обновить с помощью Kaspersky Security Center:

Список приложений сторонних производителей может обновляться и увеличиваться за счет новых приложений. Вы можете проверить, можете ли вы обновить приложение сторонних производителей (установленное на устройствах пользователей) с помощью Kaspersky Security Center, просмотрев список доступных обновлений в Kaspersky Security Center Web Console (см. стр. 675).

- 7-Zip Developers: 7-Zip.
- Adobe Systems:
  - Adobe Acrobat DC;
  - Adobe Acrobat Reader DC;
  - Adobe Acrobat;
  - Adobe Reader;
  - Adobe Shockwave Player.
- AIMPDevTeam: AIMP.
- ALTAP: Altap Salamander.
- Apache Software Foundation: Apache Tomcat.
- Apple:
  - Apple iTunes;
  - Apple QuickTime.
- Armory Technologies, Inc.: Armory.
- Cerulean Studios: Trillian Basic.
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber.
- Code Sector:
- Codec Guide:
  - K-Lite Codec Pack Basic;
  - K-Lite Codec Pack Full;
  - K-Lite Codec Pack Mega;
  - K-Lite Codec Pack Standard.
- DbVis Software AB:
- Decho Corp.:
  - Mozy Enterprise;
  - Mozy Home;
  - Mozy Pro.
- Dominik Reichl: KeePass Password Safe.
- Don HO don.h@free.fr: Notepad++.

- DoubleGIS: 2GIS.
- Dropbox, Inc.: Dropbox.
- EaseUs: EaseUS Todo Backup Free.
- Electrum Technologies GmbH:
- Enter Srl: Iperius Backup.
- Eric Lawrence:
- EverNote: EverNote.
- Exodus Movement Inc: Exodus.
- EZB Systems:
- Famatech:
  - Radmin;
  - Remote Administrator.
- Far Manager: FAR Manager.
- FastStone Soft: FastStone Image Viewer.
- FileZilla Project:
- Firebird Developers:
- Foxit Corporation:
  - Foxit Reader;
  - Foxit Reader Enterprise.
- Free Download Manager.ORG: Free Download Manager.
- GIMP project:
- GlavSoft LLC.: TightVNC.
- GNU Project: Gpg4win.
- Google:
  - Google Earth;
  - Google Chrome;
  - Google Chrome Enterprise;
  - Google Earth Pro.
- Inkscape Project:
- IrfanView: IrfanView.
- iterate GmbH:
- Logitech: SetPoint.
- LogMeIn, Inc.:
  - LogMeIn;
  - Hamachi;

  - LogMeIn Rescue Technician Console.
- Martin Prikryl:
- Mozilla Foundation:
  - Mozilla Firefox;
  - Mozilla Firefox ESR;
  - Mozilla SeaMonkey;
  - Mozilla Thunderbird.
- New Cloud Technologies Ltd: Home Edition.
- OpenOffice.org: OpenOffice.
- Opera Software: Opera.
- Oracle Corporation:
  - Oracle Java JRE;
  - Oracle VirtualBox.
- PDF44: PDF24 MSI/EXE.
- Piriform:
  - CCleaner;
  - Defraggler;
  - Recuva;
  - Speccy.
- Postgresql: PostgreSQL.
- RealPlayer Cloud.
- RealVNC:
  - RealVNC Server;
  - RealVNC Viewer.
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum).
- Simon Tatham:
- Skype Technologies: Skype for Windows.
- Sober Lemur S.a.s.:
  - PDFsam Basic;
  - PDFsam Visual.
- Softland: FBackup.
- Splashtop Inc.: Splashtop Streamer.
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP.
- Sublime HQ Pty Ltd: Sublime Text.
- TeamViewer GmbH:

  - TeamViewer Host;
  - TeamViewer.
- Telegram Messenger LLP: Telegram Desktop.
- The Document Foundation:
  - LibreOffice;
  - LibreOffice HelpPack.
- The Git Development Community:
  - Git for Windows;
  - Git LFS.
- The Pidgin developer community:
- TortoiseSVN Developers:
- VLC media player.
- VMware:
  - VMware Player;
  - VMware Workstation.
- WinRAR Developers: WinRAR.
- WinZip: WinZip.
- Wireshark Foundation: Wireshark.
- Wrike: Wrike.
- Zimbra: Zimbra Desktop.

См. также:

Сценарий: обновление приложений сторонних производителей 673
Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702
Об обновлениях приложений сторонних производителей..... 672

Сценарий: управление приложениями

Вы можете управлять запуском приложений на пользовательских устройствах. Вы можете разрешить или запретить запуск приложений на управляемых устройствах. Эта функциональность реализуется компонентом Контроль приложений. Вы можете управлять приложениями, установленными на устройствах под управлением Windows или Linux.

Для операционных систем Linux компонент Контроль приложений 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 приложений состоит из следующих этапов:

1. Формирование и просмотр списка приложений на клиентских устройствах

   Этот этап помогает вам определить, какие программы установлены на управляемых устройствах. Вы можете просмотреть список приложений и решить, какие приложения 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 приложения установлены на управляемых устройствах.

   Инструкция: Получение и просмотр списка приложений, установленных на клиентских устройствах (см. стр. 657).

2. **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. 658)

3. **Создание категорий приложений для приложений, используемых в вашей организации**

   Проанализируйте списки приложений и исполняемых файлов, хранящихся на управляемых устройствах. На основании анализа создайте категории приложений. Рекомендуется создать категорию "Рабочие приложения", которая охватывает стандартный набор приложений, используемых в вашей организации. Если разные группы безопасности используют разные наборы приложений в своей работе, для каждой группы безопасности можно создать отдельную категорию приложений.

   В зависимости от набора критериев для создания категории приложений вы можете создавать категории приложений двух типов.

   Инструкция: Создание пополняемой вручную категории приложений (см. стр. 659), Создание категории приложений, в которую входят исполняемые файлы с выбранных устройств (см. стр. 663).

4. **Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security**

   Настройте компонент Контроль приложений в политике Kaspersky Endpoint Security для Linux с использованием категорий приложений, которые вы создали на предыдущем этапе.

   Инструкция: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (см. стр. 667).

5. **Включение компонента Контроль приложений в тестовом режиме**

   Чтобы правила Контроля приложений не блокировали приложения, необходимые для работы пользователей, рекомендуется включить тестирование правил Контроля приложений и проанализировать их работу после создания правил. Когда тестирование включено, Kaspersky Endpoint Security для Windows не будет блокировать приложения, запуск которых запрещен

правилами Контроля приложений, а вместо этого будет отправлять уведомления об их запуске на Сервер администрирования.

При тестировании правил Контроля приложений 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 приложений.

Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (см. стр. 667). Следуйте этой инструкции и включите параметр **Тестовый режим** в процессе настройки.

6. **Изменение параметров категорий приложений компонента Контроль приложений**

   Если требуется, измените параметры компонента Контроль приложений. На основании результатов тестирования вы можете добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений пополняемую вручную.

   Инструкции для Kaspersky Security Center Web Console: Добавление исполняемых файлов, связанных с событием, в категорию приложения (см. стр. 669).

7. **Применение правил Контроля приложений в рабочем режиме**

   После проверки правил Контроля приложений и завершения настройки категорий приложений вы можете применить правила Контроль приложений в рабочем режиме.

   Инструкции для Kaspersky Security Center Web Console: Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows (см. стр. 667). Следуйте этой инструкции и выключите параметр **Тестовый режим** в процессе настройки.

8. **Проверка конфигурации Контроля приложений**

   Убедитесь, что вы выполнили следующее:

   - Создали категории приложений.
   - Настроили Контроль приложений с использованием категорий приложений.
   - Применили правила Контроля приложений в рабочем режиме.

Результаты

После завершения сценария, запуск приложений на управляемых устройствах контролируется. Пользователи могут запускать только те приложения, которые разрешены в вашей организации, и не могут запускать приложения, запрещенные в вашей организации.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

О Контроле приложений

Компонент Контроль приложений контролирует попытки пользователей запуска приложений и регулирует запуск приложений с помощью правил Контроля приложений.

kaspersky

Компонент Контроль приложений доступен для версии приложения Kaspersky Endpoint Security 11.2 для Linux и выше.

Запуск приложений, параметры которых не соответствуют ни одному из правил Контроля приложений, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех приложений, кроме приложений, указанных в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите заблокировать запуск всех приложений, кроме приложений, указанных в разрешающих правилах.

Правила Контроля приложений реализуются с помощью категорий приложений. Вы создаете категории приложений с определенными критериями. В Kaspersky Security Center существует три типа категорий приложений:

- Пополняемая вручную категория. (см. стр. 659) 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. 663). Вы указываете устройство, исполняемые файлы которого автоматически включаются в категорию.
- Категория, в которую входят исполняемые файлы из выбранных папок (см. стр. 664). Вы указываете папку, исполняемые файлы из которой автоматически попадают в категорию.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

Получение и просмотр списка приложений, 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 приложений, установленных на устройстве, и передает список Серверу администрирования. Агенту администрирования требуется около 10–15 минут для обновления списка приложений.

Для клиентских устройств с операционной системой Windows Агент администрирования получает большую часть информации об установленных приложениях из реестра Windows. Для клиентских устройств с операционной системой Linux информацию об установленных приложениях Агент администрирования получает от диспетчеров пакетов.

► *Чтобы просмотреть список приложений, установленных на управляемых устройствах,*

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Реестр приложений**.

   На странице отображается таблица с приложениями, установленными на управляемых устройствах. Выберите приложение, чтобы просмотреть свойства этого приложения, например: имя

производителя, номер версии, список исполняемых файлов, список устройств, на которых установлено приложение.

2. Вы можете группировать и фильтровать данные таблицы с установленными приложениями 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 установлено приложение, 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 приложений.

Чтобы просмотреть список приложений, установленных на выбранном управляемом устройстве,

В главном окне приложения перейдите в раздел **Устройства** → **Управляемые устройства** → **<имя устройства>** → **Дополнительно** → **Реестр приложений**. В этом меню можно экспортировать список приложений в файлы форматов CSV или TXT.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

См. также:

Сценарий: управление приложениями 654

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вам нужно создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для приложения Kaspersky Endpoint Security для Linux версии 11.2 и выше.

► *Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:*

1. В главном окне приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи (см. стр. 454). Следуйте далее указаниям мастера.

3. На странице **Новая задача** в раскрывающемся списке **Приложение** 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 справке Kaspersky Endpoint Security для Linux https://support.kaspersky.com/KES4Linux/11.3.0/ru-RU/245017.htm и Kaspersky Endpoint Security для Windows https://support.kaspersky.com/KESWin/12.3/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 приложение обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML-файлы.

► *Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,*

В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

См. также:

Сценарий: управление приложениями 654

Создание пополняемой вручную категории приложений

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 приложений и использовать ее в настройке компонента Контроль приложений.

► *Чтобы создать пополняемую вручную категорию приложений:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

   Откроется страница со списком категорий приложений.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории приложений и выберите параметр **Пополняемая вручную категория. Данные об исполняемых файлах добавляются в категорию вручную**.
4. На шаге **Условия** нажмите на кнопку **Добавить**, чтобы добавить критерий условия для включения файлов в создаваемую категорию.
5. На шаге **Критерии условия** выберите тип правила для создания категории из списка:
   - **Из KL-категории**

     Если выбран этот вариант, в качестве условия добавления приложений в пользовательскую категорию можно указать категорию приложений "Лаборатории Касперского". Приложения, входящие в указанную KL-категорию, будут добавлены в пользовательскую категорию приложений.
   - **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 приложению (поддерживаются маски)**

     Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию приложений.
   - **Съемный диск**

     Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск приложения. Приложения, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию приложений.
   - **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:
     - **Выберите из списка исполняемых файлов.**

       Если выбран этот вариант, приложения для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.
     - **Выберите из реестра приложений.**

Если выбран этот параметр, отображается реестр приложений. Вы можете выбрать приложения 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 приложения.
- Версия приложения. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
- Производитель.
  - **Задайте вручную**

    Если выбран этот вариант, вам нужно указать хеш файла, метаданные или сертификат в качестве условия добавления приложений в пользовательскую категорию.

Хеш файла

В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением 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.

SHA256 – 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 SHA256.

Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

- Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.
- 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 приложений.

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 приложений 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 SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  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 приложений.

- **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 приложений 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 SHA256) вы хотите использовать для вычисления значения хеш-функции. Приложения, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию приложений.

  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 приложений.

- **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 приложений, сколько вам нужно.

1. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.
2. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

См. также:

Сценарий: управление приложениями 654

kaspersky

Создание категории приложений, 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 приложений и использовать ее для настройки компонента Контроль приложений.

► *Чтобы создать категорию приложений, в которую входят исполняемые файлы с выбранных устройств:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Категории приложений**.

   Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **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 приложений.

6. Задайте следующие параметры:

   - Алгоритм вычисления хеш-функции

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением 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.

     SHA256 – 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 SHA256.

     Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

     - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.

     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 SHA256 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 приложений.

  Все файлы. Для создаваемой категории учитываются все файлы. По умолчанию выбран этот вариант.

  Только файлы вне категорий приложений. Для создаваемой категории учитываются только файлы вне категорий приложений.

- **Папки**

В этом разделе вы можете указать папки выбранных устройств, содержащие файлы, которые используются для создания категории приложений.

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, вам нужно указать путь к папке.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете создать категорию приложений при настройке компонента Контроль приложений.

См. также:

Сценарий: управление приложениями 654

Создание категории приложений, в которую входят исполняемые файлы из выбранных папок

Вы можете использовать исполняемые файлы выбранных папок как эталонный набор исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов из выбранных папок вы можете создать категорию приложений и использовать ее для настройки компонента Контроль приложений.

► *Чтобы создать категорию приложений, в которую входят исполняемые файлы из выбранных папок:*

1. В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Категории приложений**.

Откроется страница со списком категорий приложений.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории**, укажите имя категории и выберите параметр **Категория, в которую входят исполняемые файлы с выбранных устройств. Исполняемые файлы приложений копируются в указанную папку, обрабатываются автоматически, и их метрики заносятся в категорию**.

4. Укажите папку, исполняемые файлы которой будут использоваться для создания категории приложений.

5. Настройте следующие параметры:

   - **Включать в категорию динамически подключаемые библиотеки (DLL)**

     В категорию приложений включаются динамически подключаемые библиотеки (файлы формата DLL), и компонент Контроль приложений регистрирует действия таких библиотек, запущенных в системе. При включении файлов формата DLL в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Включать в категорию данные о скриптах**

     В категорию приложений включаются данные о скриптах, и скрипты не блокируются компонентом Защита от веб-угроз. При включении данных о скриптах в категорию возможно снижение производительности работы Kaspersky Security Center.

     По умолчанию флажок снят.

   - **Алгоритм вычисления хеш-функции**: **Вычислять SHA256 для файлов в категории (поддерживается для версии Kaspersky Endpoint Security 10 Service Pack 2 для Windows и выше) / Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)**

     В зависимости от версии приложения безопасности, установленного на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции приложением 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.

     SHA256 – 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 SHA256.

     Выберите один из вариантов вычисления хеш-функции приложением Kaspersky Security Center для файлов категории:

     - Если все экземпляры приложений безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA256**.

     Установите флажок **MD5 хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

     По умолчанию флажок **Вычислять SHA256 для файлов в категории (поддерживается для Kaspersky Endpoint Security 10 Service Pack 2 для**

Windows и выше) установлен.

По умолчанию флажок **Вычислять MD5 для файлов в категории (поддерживается для версий ниже Kaspersky Endpoint Security 10 Service Pack 2 для Windows)** снят.

- **Принудительно проверять папку на наличие изменений**

  Если этот параметр включен, приложение периодически принудительно проверяет папку пополнения категорий на наличие изменений. Периодичность проверки в часах можно указать в поле ввода рядом с флажком. По умолчанию период принудительной проверки равен 24 часам.

  Если этот параметр выключен, принудительная проверка папки не выполняется. Сервер обращается к файлам в папке в случае их изменения, добавления или удаления.

  По умолчанию параметр выключен.

После завершения мастера создается категория приложений. Оно появится в списке категорий приложений. Вы можете использовать категорию приложений для настройки компонента Контроль приложений.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

См. также:

Сценарий: управление приложениями 654

Просмотр списка категорий приложений

Вы можете просмотреть список настроенных категорий приложений и параметры каждой категории приложений.

► *Чтобы просмотреть список категорий приложений,*

В главном окне приложения перейдите в раздел **Операции → Приложения сторонних производителей → Категории приложений**.

Откроется страница со списком категорий приложений.

► *Чтобы просмотреть свойства категории приложений,*

нажмите на имя категории приложений.

Откроется окно свойств выбранной категории приложений. Параметры сгруппированы на нескольких вкладках.

См. также:

Сценарий: управление приложениями 654

Настройка компонента Контроль приложений в политике Kaspersky Endpoint Security для Windows

После создания категорий для Контроля приложений, вы можете использовать их для настройки Контроля приложений в политиках Kaspersky Endpoint Security для Windows.

► *Чтобы настроить компонент Контроль приложений в политике Kaspersky Endpoint Security для Windows:*

1. В главном окне приложения 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 приложения** → **Контроль безопасности** → **Контроль приложений**.

   Отобразится окно **Контроль приложений** с параметрами компонента Контроль приложений.

4. Параметр **Контроль приложений** включен по умолчанию. Выключите переключатель **Контроль приложений [Выключен]**, чтобы выключить параметр.

5. В блоке **Параметры Контроля приложений** включите режим работы с применением правил Контроля приложений и разрешите Kaspersky Endpoint Security для Windows блокировку запуска приложений.

   Если вы хотите протестировать правила Контроля приложений, в разделе **Параметры Контроля приложений**, включите тестовый режим. В тестовом режиме Kaspersky Endpoint Security для Windows не блокирует запуск приложений, 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 приложение Kaspersky Endpoint Security для Windows контролировало загрузку модулей DLL при запуске приложений пользователями.

   Информация о модуле и приложении, которое загрузило 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 приложение Kaspersky Endpoint Security для Windows контролировало 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 приложение заблокировано для запуска, и шаблон сообщения электронной почты, которое отправляется вам.

8. В блоке параметров **Режим Контроля приложений** 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 приложений. 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 приложений**.

11. Перейдите по ссылке **Пожалуйста, выберите категорию**.

    Откроется окно **Категории приложений**.

12. Добавьте категорию приложений (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 приложений завершено, нажмите кнопку **ОК**.

    Окно **Категории приложений** закрывается.

14. В окне правил **Контроль приложений** в разделе **Субъекты и их права** создайте список пользователей и групп пользователей, чтобы применить к ним правила Контроля приложений.

15. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Правило Контроля приложений**.

16. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Списки запрещенных и разрешенных**.

17. Нажмите на кнопку **ОК**, чтобы сохранить параметры и закрыть окно **Контроль приложений**.

18. Закройте окно с параметрами политики Kaspersky Endpoint Security для Windows.

Компонент Контроль приложений настроен. После распространения политики на клиентские устройства запуск исполняемых файлов контролируется.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

См. также:

Сценарий: управление приложениями 654

kaspersky

Добавление исполняемых файлов, связанных с событием, в категорию приложений

После настройки компонента Компонента Контроль приложений в политиках Kaspersky Endpoint Security в списке событий могут отображаться следующие события:

- **Запуск приложения запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил.
- **Запуск приложения запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль приложений для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска приложения** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль приложений для применения правил, а пользователь запросил доступ к приложению, которое заблокировано для запуска.

Рекомендуется создавать выборки событий (см. стр. 590) для просмотра событий, связанных с компонентом Контроль приложений.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля приложений, в существующую категорию приложений или в новую категорию приложений. Вы можете добавлять исполняемые файлы только в категорию приложений пополняемую вручную.

► *Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль приложений, в категорию приложений:*

1. В главном окне приложения перейдите в раздел **Мониторинг и отчеты → Выборки событий**.

   Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем приложений, и запустите формирование этой выборки событий (см. стр. 591).

   Если вы не создали выборку событий, связанную с Контролем приложений, 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 приложений, 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 приложений**

       Выберите этот параметр, если вы хотите создать категорию приложений 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 приложений.

По умолчанию вариант не выбран.

Если вы выбрали этот параметр, выберите категорию приложений, 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 SHA256 для файлов без сертификата**

    Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений одного производителя.

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию SHA256 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 одного приложения могут быть подписаны одним сертификатом или несколько разных приложений одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий приложения или несколько приложений 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 SHA256 (файлы без хеша пропускаются)**

    Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия приложения.

    Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 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 приложения.

1. Нажмите на кнопку **ОК**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля приложений, добавляются в существующую категорию приложений или в новую категорию приложений. Вы можете просмотреть параметры категории приложений, которую вы изменили или создали.

Подробнее о Контроле приложений 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/12.3/ru-RU/127971.htm.

См. также:

Установка обновлений приложений сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center, относящиеся к установке обновлений для приложений сторонних производителей, установленных на клиентских устройствах.

В этом разделе

kaspersky

Об обновлениях приложений сторонних производителей

Kaspersky Security Center позволяет управлять обновлениями стороннего программного обеспечения, установленного на управляемых устройствах, и закрывать уязвимости в таких приложениях путем установки требуемых обновлений.

Kaspersky Security Center выполняет поиск обновлений с помощью задачи *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Сервер администрирования получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах. После просмотра информации о доступных обновлениях вы можете выполнить установку обновлений на ваши устройства.

Обновление некоторых приложений Kaspersky Security Center выполняет путем удаления предыдущей версии приложения и установки новой версии.

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

Когда метаданные обновлений стороннего программного обеспечения загружаются в хранилище, вы можете установить обновления на клиентские устройства, выполнив задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689).

> Задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689) можно создать, только если у вас есть лицензия на Системное администрирование.

После завершения работы этой задачи обновления устанавливаются на управляемые устройства автоматически. При загрузке метаданных новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли обновления критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут загружены и установлены автоматически при следующем запуске задачи.

kaspersky

Сценарий: обновление приложений сторонних производителей

В этом разделе представлен сценарий обновления приложений сторонних производителей, установленных на клиентских устройствах. Приложения сторонних производителей включают в себя приложения от других поставщиков программного обеспечения (см. стр. 650).

Предварительные требования

Сервер администрирования должен быть подключен к интернету для установки обновлений стороннего программного обеспечения.

Этапы

Обновление производителей состоит из следующих этапов:

1. Поиск требуемых обновлений

   Чтобы найти обновления приложений сторонних производителей, необходимые для управляемых устройств, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для программ сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

   Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center Сервера администрирования. Если вы не запустили мастер, создайте задачу *Поиск уязвимостей и требуемых обновлений* (см. стр. 682) или запустите мастер первоначальной настройки.

   > Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

2. **Просмотр списка найденных обновлений**

   Просмотрите информацию о доступных обновлениях стороннего программного обеспечения (см. стр. 686) и решите, какие обновления вы хотите установить. Чтобы просмотреть подробную информацию о каждом обновлении, нажмите на имя обновления в списке. Для каждого обновления в списке также можно просмотреть статистику установки обновлений на клиентских устройствах.

3. **Настройка установки обновлений**

   После того как Kaspersky Security Center получает список обновлений приложений сторонних производителей, вы можете установить их на клиентские устройства, создав задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689).

   > Вы можете создать задачу *Установка требуемых обновлений и закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

   Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для установки обновлений для программ Microsoft, включая обновления, предоставляемые службой Центра обновления Windows, и обновления программ других поставщиков. Обратите внимание, что задачу *Установка требуемых обновлений* и закрытие уязвимостей можно создать, только если у вас есть лицензия на Системное администрирование.

Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение для установки программного обеспечения. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не будут установлены.

Вы можете запустить задачу установки обновления по расписанию. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

4. **Задание расписания задачи**

   Чтобы убедится, что список обновлений всегда актуален, задайте расписание запуска задачи *Поиск уязвимостей и требуемых обновлений*, чтобы она периодически запускалась автоматически. По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Одобрение и отклонение обновлений приложений сторонних производителей (необязательно)**

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете указать правила установки обновлений в свойствах задачи.

   Для каждого правила вы можете выбрать устанавливаемые обновления в зависимости от их статуса: *Не определено*, *Одобрено* или *Отклонено*. Например, вы можете создать определенную задачу для серверов и установить правило для этой задачи, чтобы разрешить установку только тех обновлений, которые имеют статус *Подтверждено*. После этого вы вручную устанавливаете статус *Одобрено* для тех обновлений, которые вы хотите установить. В этом случае обновления со статусом *Не определено* или *Отклонено* не будут установлены на серверы, указанные в задаче.

   При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в задаче *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. Если вы подтверждаете вручную большое количество обновлений, производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

   По умолчанию загруженные обновления программного обеспечения имеют статус *Не определено*. Вы можете изменить статус на *Одобрено* или *Отклонено* в списке **Обновления программного обеспечения** (**Операции** → **Управление патчами** → **Обновления программного обеспечения**).

   Дополнительные сведения см. в инструкциях по одобрению и отклонению обновлений стороннего программного обеспечения (см. стр. 688).

6. **Запуск задачи установки обновлений**

   Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*. После запуска этой задачи, обновления загружаются и устанавливаются на управляемые устройства. После завершения задачи убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создать отчет о результатах установки обновления (необязательно)**

   Чтобы просмотреть статистику установки обновления, сформируйте отчет о результатах установки обновлений стороннего ПО (см. стр. 561).

Результаты

Если вы создали и настроили задачу *Установка требуемых обновлений и закрытия уязвимостей*, обновления будут автоматически установлены на управляемые устройства. При загрузке новых обновлений в хранилище Сервера администрирования Kaspersky Security Center проверяет, соответствуют ли они критериям, указанным в правилах обновлений. Все новые обновления, которые соответствуют критериям, будут установлены автоматически при следующем запуске задачи.

См. также

Варианты установки обновлений стороннего программного обеспечения

Вы можете установить обновления стороннего программного обеспечения и обновления из Центра обновления Windows на управляемые устройства, создав и запустив задачу *Установка требуемых обновлений и закрытие уязвимостей (см. стр. 689)*. Задачу *Установка требуемых обновлений и закрытие уязвимостей* можно создать, только если у вас есть лицензия на Системное администрирование. Вы можете использовать эту задачу для установки обновлений приложений сторонних производителей (см. стр. 650).

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для установки необходимых обновлений следующими способами:

- Открыть список обновлений и указать, какие обновления устанавливать.

В результате создается задача для установки выбранных обновлений. Также вы можете добавить выбранные обновления в существующую задачу.

- Запустить мастер установки обновлений.

  Мастер установки обновлений доступен при наличии лицензии на Системное администрирование (см. стр. 370).

  Мастер упрощает создание и настройку задачи установки обновлений и позволяет исключить создание избыточных задач, содержащих те же самые обновления для установки.

Установка обновлений приложений сторонних производителей с помощью списка обновлений

► *Чтобы установить обновления приложений сторонних производителей:*

1. Откройте список обновлений, одним из следующих способов:
   - **Операции** → **Управление патчами** → **Обновления программного обеспечения**.
   - **Активы (Устройства)** → **Управляемые устройства** → <имя устройства> → **Дополнительно** → **Применимые обновления**.
   - **Операции** → **Обновления сторонних приложений** → **Реестр приложений** → <имя приложения> → **Применимые обновления**.

   Отобразится список доступных обновлений.
2. Установите флажки рядом с теми обновлениями, которые вы хотите установить.
3. Нажмите на кнопку **Установить обновления**. Если эта кнопка не отображается, нажмите на кнопку с многоточием и в раскрывающемся списке выберите пункт **Установить обновления**.

   Для установки некоторых обновлений программного обеспечения вам нужно принять Лицензионное соглашение. Если вы отклоните Лицензионное соглашение, обновления программного обеспечения не установятся.
4. Выберите один из следующих вариантов:
   - **Новая задача.**

     Запустится мастер создания задачи (см. стр. 454). Если у вас есть лицензия на Системное администрирование (см. стр. 370), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.
   - **Установить обновление (добавить правило в указанную задачу)**

     Выберите задачу, в которую вы хотите добавить выбранные обновления. Если у вас есть лицензия на Системное администрирование (см. стр. 370), выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу автоматически добавлено правило для закрытия выбранных уязвимостей. Выбранные обновления добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление обновлений в существующую задачу, обновления сохраняются в свойствах задачи.

Для установки обновлений стороннего программного обеспечения необходимо запустить задачу *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете запустить эту задачу, нажав на кнопку **Запустить** в списке задач или указав параметры расписания в свойствах задачи, которую вы запускаете. При указании расписания задачи убедитесь, что задача установки обновления запускается после завершения задачи *Поиск уязвимостей и требуемых обновлений*.

Установка обновлений приложений сторонних производителей с помощью мастера установки обновлений

Мастер установки обновлений доступен при наличии лицензии на Системное администрирование (см. стр. 370).

► *Чтобы создать задачу установки обновлений приложений сторонних производителей с помощью мастера установки обновления:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.
2. Установите флажок рядом с обновлением, которое вы хотите установить.
3. Нажмите на кнопку **Запустить мастер установки обновления**.

   Запустится мастер установки обновления. На странице **Выбор задачи установки обновления** отображается список всех существующих задач следующих типов:

   - *Установка требуемых обновлений и закрытия уязвимостей.*
   - *Закрытие уязвимостей.*
4. Если вы хотите, чтобы мастер отображал только те задачи, которые устанавливают выбранное вами обновление, включите параметр **Показать только задачи, которые устанавливают обновление**.
5. Выберите действие, которое хотите выполнить:

   - Чтобы запустить существующую задачу, установите флажок рядом с задачей *Установка требуемых обновлений и закрытие уязвимостей* и нажмите на кнопку **Запуск**.

     Задача выполняется в фоновом режиме. Никаких дальнейших действий не требуется.
   - Чтобы добавить новое правило в существующую задачу:

     a. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Добавить правило**.

     Кнопка **Добавить правило** недоступна, если вы выбрали более одной задачи.

     Вы не можете добавить правило для задачи *Закрытие уязвимостей*. Если вы выбрали задачу *Закрытие уязвимостей*, появится следующее уведомление: "*Для установки обновлений используйте задачу "Установка требуемых обновлений и закрытие уязвимостей*"".

     b. На шаге мастера **Создание правила установки обновления** настройте новое правило:

     - **Правило установки обновлений данного уровня важности**

Это правило не отображается, если уровень важности выбранного обновления – *Неизвестно*.

- **Правило установки обновлений данного уровня важности по MSRC**

Это правило отображается только для обновлений программного обеспечения Microsoft. Правило не отображается, если уровень важности выбранного обновления – *Неизвестно*.

- **Правило установки обновлений данного поставщика**

Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки обновлений типа**
- **Правило установки обновлений выбранного приложения**

Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки выбранного обновления**
- **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

a. Нажмите на кнопку **Добавить**.

Откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

- Чтобы создать задачу:

  a. Нажмите на кнопку **Новая задача**.

  b. На шаге мастера **Создание правила установки обновления** настройте новое правило:

  - **Правило установки обновлений данного уровня важности**

  Это правило не отображается, если уровень важности выбранного обновления – *Неизвестно*.

  - **Правило установки обновлений данного уровня важности по MSRC**

Это правило отображается только для обновлений программного обеспечения Microsoft. Правило не отображается, если уровень важности выбранного обновления – *Неизвестно*.

- **Правило установки обновлений данного поставщика**

Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки обновлений типа**
- **Правило установки обновлений выбранного приложения**

Это правило отображается только для обновлений стороннего программного обеспечения.

- **Правило установки выбранного обновления**
- **Одобрить выбранные обновления**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

- **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

  Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

  Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

  Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

  По умолчанию параметр включен.

a. Нажмите на кнопку **Добавить**.

Продолжите создавать задачу в мастере создания задачи (см. стр. 689). Новое правило, добавленное вами в мастере установки обновлений, отображается в мастере создания задачи. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Параметры задачи поиска уязвимостей и требуемых обновлений

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки. Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную (см. стр. 682).

Помимо общих параметров задачи (см .стр. 456), вы можете указать следующие параметры при создании задачи *Поиск уязвимостей и требуемых обновлений* или позже, при настройке свойств созданной задачи:

- **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Подключаться к серверу обновлений для получения новых данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

  Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

  Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

  По умолчанию параметр включен.

  Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

  - Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
  - Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединяться с сервером**

обновлений для актуализации данных выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.

- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**, Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Укажите способ дополнительного поиска приложений в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

  При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

  По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную. Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (утром следующего дня). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

См. также:

Сценарий: настройка защиты сети.....393

Сценарий: обновление приложений сторонних производителей 673

Создание задачи Поиск уязвимостей и требуемых обновлений

С помощью задачи *Поиск уязвимостей и требуемых обновлений* Kaspersky Security Center получает списки обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, установленных на управляемых устройствах.

Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

Задача *Поиск уязвимостей и требуемых обновлений* создается автоматически во время работы мастера первоначальной настройки (см. стр. 143). Если вы не запускали мастер первоначальной настройки, вы можете создать задачу вручную.

► *Чтобы создать задачу Поиск уязвимостей и требуемых обновлений:*

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

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для приложения Kaspersky Security Center выберите тип задачи **Поиск уязвимостей и требуемых обновлений**.
4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Укажите способы проверки уязвимостей и приложений, требующих обновления:
   - **Поиск уязвимостей и обновлений, перечисленных Microsoft**

При поиске уязвимостей и обновлений Kaspersky Security Center использует данные о применимых обновлениях Microsoft из источника обновлений Microsoft, доступного в текущий момент.

Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft и обновлений сторонних приложений.

По умолчанию параметр включен.

- **Подключаться к серверу обновлений для получения новых данных**

  Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft. Следующие службы могут выступать в качестве источника обновлений Microsoft:

  - Сервер администрирования Kaspersky Security Center (см. параметры политики Агента администрирования).
  - Windows Server со службами Microsoft Windows Server Update Services (WSUS), развернутыми в сети вашей организации.
  - Серверы обновления Microsoft.

Если этот параметр включен, Агент Центра обновления Windows на управляемом устройстве подключается к источнику обновлений Microsoft и получает информацию о применимых обновлениях Microsoft Windows.

Если этот параметр выключен, Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, которую он получил из источника обновлений Microsoft ранее и которая хранится в кеше устройства.

Подключение к источнику обновлений Microsoft может оказаться ресурсоемким. Вы можете выключить этот параметр, если у вас установлено регулярное подключение к этому источнику обновлений в другой задаче или в свойствах политики Агента администрирования, в разделе **Обновления и уязвимости в приложениях**. Если вы не хотите выключать этот параметр, то, чтобы уменьшить нагрузку на Сервер, вы можете настроить расписание задач так, чтобы использовать случайное значение задержки запуска задачи в интервале 360 минут.

По умолчанию параметр включен.

Комбинация следующих значений параметров политики Агента администрирования определяет режим получения обновлений:

- Агент Центра обновления Windows на управляемом устройстве подключается к серверу обновлений Microsoft, чтобы получить обновления, только если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Активный** в группе параметров **Режим поиска Центра обновления Windows**.
- Агент Центра обновления Windows на управляемом устройстве использует информацию о применимых обновлениях Microsoft Windows, полученную ранее от источника обновлений Microsoft и сохраненную в кеше устройства, если включен параметр **Соединяться с сервером обновлений для актуализации данных** и параметр **Пассивный** в группе параметров **Режим поиска Центра обновления Windows**, или если параметр **Соединяться с сервером обновлений для актуализации данных** выключен, а в группе параметров **Режим поиска Центра обновления Windows** выбран параметр **Активный**.
- Независимо от параметра **Соединяться с сервером обновлений для актуализации данных** (включен он или выключен), если в группе параметров **Выключен** выбран параметр **Режим поиска Центра обновления Windows**,

Kaspersky Security Center не запрашивает информацию об обновлениях.

- **Поиск уязвимостей и обновлений сторонних производителей, перечисленных "Лабораторией Касперского"**

Если этот параметр включен, Kaspersky Security Center выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) в реестре Windows и в папках, указанных в разделе **Укажите пути для дополнительного поиска приложений в файловой системе**. Полный список поддерживаемых приложений сторонних производителей контролируется "Лабораторией Касперского".

Если этот параметр выключен, Kaspersky Security Center не выполняет поиск уязвимостей и требуемых обновлений для приложений сторонних производителей. Например, можно выключить этот параметр, если имеются различные задачи с различными параметрами для обновлений Microsoft Windows и обновлений сторонних приложений.

По умолчанию параметр включен.

Вы можете выключить эти параметры после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

1. **Укажите способ дополнительного поиска приложений в файловой системе**

Папки, в которых Kaspersky Security Center выполняет поиск сторонних приложений, требующих закрытия уязвимостей и установки обновлений. Вы можете использовать системные переменные.

Укажите папки, в которые были установлены приложения. По умолчанию список содержит системные папки, в которые устанавливается большинство приложений.

Вы можете изменить указанные пути после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

1. При необходимости **Включить расширенную диагностику**

   Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

   Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

   При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

   По умолчанию параметр выключен.

   Вы можете выключить этот параметр после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

2. Укажите **Максимальный размер файлов расширенной диагностики, МБ.**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Вам нужно указать это значение, если вы включили расширенную диагностику на предыдущем шаге. Вы можете изменить это значение после создания задачи на вкладке **Параметры приложения** в окне свойств задачи.

1. 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.
2. Нажмите на кнопку **Готово**.

   В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо (см. стр. 456).

   Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

Задача создана и настроена. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Рекомендации по настройке расписания запуска задачи

При планировании расписания запуска задачи *Поиск уязвимостей и требуемых обновлений* убедитесь, что включены два параметра **Запускать пропущенные задачи** и **Использовать автоматическое определение случайного интервала между запусками задачи**.

По умолчанию задача *Поиск уязвимостей и требуемых обновлений* запускается в 18:00:00 вручную.

Вы также можете настроить расписание запуска задачи *Поиск уязвимостей и требуемых обновлений* в определенное время. Например, вы можете выбрать запуск по расписанию **Ежедневно (не поддерживается переход на летнее время)** из раскрывающегося списка **Запуск задачи** на вкладке **Расписание** окна свойств задачи. В этом случае, если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства. Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. стр. 456).

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....702

Сценарий: обновление приложений сторонних производителей 673

kaspersky

Просмотр информации о доступных обновлениях приложений сторонних производителей.

Вы можете просмотреть список доступных обновлений для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на клиентских устройствах.

► *Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на клиентских устройствах,*

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

Отобразится список доступных обновлений.

Вы можете указать фильтр для просмотра списка обновлений приложений. Нажмите на значок **Фильтр** () в списке обновлений приложений для управления фильтром. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

► *Чтобы просмотреть свойства обновления:*

1. Нажмите на имя требуемого обновления программного обеспечения.
2. Откроется окно свойств обновления, в котором отображается следующая информация, сгруппированная по вкладкам:
   - **Общие**
   - **Атрибуты**
   - **Устройства**
   - **Закрываемые уязвимости**
   - **Пересечения обновлений**
   - **Задачи для установки обновления**

► *Чтобы просмотреть статистику установки обновления:*

1. Установите флажок рядом с требуемым обновлением.
2. Нажмите на кнопку **Статистика состояния установки обновлений**.

На диаграмме отобразится информация о статусах обновлений. При нажатии на статус открывается список устройств с выбранным статусом.

Вы можете просмотреть информацию о доступных обновлениях для приложений сторонних производителей, включая программное обеспечение Microsoft, установленных на выбранном управляемом устройстве под управлением Windows.

► *Чтобы просмотреть список доступных обновлений для приложений сторонних производителей, установленных на выбранном управляемом устройстве:*

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

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обновления приложений сторонних производителей.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.
4. На левой панели выберите раздел **Применимые обновления**. Если вы хотите просматривать только установленные обновления, включите параметр **Показывать установленные обновления**.

Отобразится список доступных обновлений приложений сторонних производителей для выбранного устройства.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Экспорт списка доступных обновлений в файл

Вы можете экспортировать список обновлений для приложений сторонних производителей, включая приложения Microsoft, в файл формата CSV или TXT. Вы можете использовать эти файлы, например, чтобы отправить их вашему начальнику по информационной безопасности или сохранить их в целях статистики.

► *Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на всех управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

   При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

   Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, загружается на ваше текущее устройство.

► *Чтобы экспортировать список доступных обновлений для приложений сторонних производителей в текстовый файл, установленных на выбранном управляемом устройстве:*

1. Откройте список доступных обновлений приложений сторонних производителей на выбранном управляемом устройстве (см. стр. 686).

   Отобразится список доступных обновлений.

При экспорте полного списка обновлений приложений, будут экспортированы только те обновления, которые отображаются на текущей странице.

Если вы хотите экспортировать только определенные обновления, установите флажки рядом с требуемыми обновлениями в списке.

Если вы хотите экспортировать только установленные обновления, установите флажок **Показывать установленные обновления**.

2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

Файл, содержащий список доступных обновлений для приложений сторонних производителей, включая приложения Microsoft, установленные на выбранных управляемых устройствах, загружается на ваше текущее устройство.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Одобрение и отклонение обновлений приложений сторонних производителей.

При настройке задачи *Установка требуемых обновлений и закрытия уязвимостей*, вы можете создать правило, для выполнения которого устанавливаемые обновления должны иметь определенный статус. Например, правило обновления может разрешить установку следующего:

- только одобренных обновлений;
- только одобренных обновлений и неопределенных обновлений;
- всех обновлений, независимо от статусов обновлений.

Вы можете подтверждать обновления, которые необходимо установить, и отклонять обновления, которые не должны быть установлены.

При управлении установкой обновлений использовать статуса *Одобрено* целесообразно для небольшого количества обновлений. Чтобы установить несколько обновлений, используйте правила, которые вы можете настроить в свойствах задачи *Установка требуемых обновлений и закрытие уязвимостей*. Рекомендуется устанавливать статус *Одобрено* только для тех обновлений, которые не соответствуют критериям, указанным в правилах. Если вы одобряете вручную большое количество обновлений, производительность Сервера администрирования снижается, что может привести к перегрузке Сервера администрирования.

► *Чтобы подтвердить или отменить одно или несколько обновлений:*

1. В главном окне приложения перейдите в раздел **Операции → Управление патчами → Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

2. Выберите обновления, которые требуется подтвердить или отклонить.

3. Нажмите на кнопку **Одобрить**, чтобы одобрить выбранное обновление, или на кнопку **Отклонить**, чтобы отклонить выбранное обновление. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

   Статус обновления по умолчанию – *Не определен*.

Выбранные обновления имеют статусы, которые вы указали.

Также вы можете изменить статус в свойствах требуемого обновления.

► *Чтобы одобрить или отклонить обновление:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Обновления программного обеспечения**.

   Отобразится список доступных обновлений.

2. Выберите обновление, которое требуется одобрить или отклонить.

   Откроется окно свойств обновления.

3. В разделе **Общие** выберите статус обновления в раскрывающемся списке **Статус одобрения обновления**. Вы можете выбрать статус *Одобрено*, *Отклонено* или *Не определено*.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Выбранное обновление имеет статус, который вы указали.

Если вы устанавливаете статус *Отклонить* для обновлений стороннего программного обеспечения, то эти обновления не будут устанавливаться на те устройства, для которых они были запланированы к установке, но еще не были установлены. Обновления останутся на тех устройствах, на которые они уже были установлены. При необходимости вы можете удалить их локально вручную.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Создание задачи Установка требуемых обновлений и закрытие уязвимостей 689

Создание задачи Установка требуемых обновлений и закрытие уязвимостей

Задача *Установка требуемых обновлений и закрытие уязвимостей* доступна при наличии лицензии на Системное администрирование (см. стр. 370).

Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с правилами, которые вы укажете в параметрах задачи.

Чтобы установить обновления или исправить уязвимости с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*, вы можете выполнить одно из следующих действий:

- Запустите мастер установки обновлений (см. стр. 675) или мастер закрытия уязвимостей (см. стр. 704).
- Создайте задачу *Установка требуемых обновлений и закрытие уязвимостей*.
- Добавьте правило для установки обновления (см. стр. 694) в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*.

► *Чтобы создать задачу Установка требуемых обновлений и закрытие уязвимостей:*

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

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center.
4. В списке **Тип задачи** выберите тип задачи **Установка требуемых обновлений и закрытие уязвимостей**.

   Если задача не отображается, проверьте, есть ли у вашей учетной записи права **Чтение**, **Запись** и **Выполнение** в функциональной области **Управление системой**: **Системное администрирование** (см. стр. 478). Вы не можете создавать и настраивать задачу *Установка требуемых обновлений и закрытие уязвимостей* без этих прав доступа.
5. В поле **Название задачи** укажите название новой задачи.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача (см. стр. 456).
7. На шаге мастера **Задайте правила установки обновлений** добавьте правила установки обновлений (см. стр. 694).

Эти правила применяются при установке обновлений на клиентские устройства. Если правила не указаны, задача не выполняется. Дополнительную информацию о работе с правилами см. в разделе Правила установки обновлений.

Эти правила применяются при установке обновлений на клиентские устройства. Если вы не укажете никаких правил, задача не будет выполняться.

1. Задайте следующие параметры:
   - **Start installation at device restart or shutdown**

     Если флажок установлен, установка обновления выполняется перед перезагрузкой или выключением устройства. В противном случае установка обновлений выполняется по расписанию.

     Установите этот флажок, если установка обновлений может повлиять на производительность устройств.

     По умолчанию параметр выключен.
   - **Устанавливать необходимые общесистемные компоненты (пререквизиты)**

     Если флажок установлен, перед установкой обновления приложение автоматически устанавливает все общесистемные компоненты (пререквизиты), необходимые для установки этого обновления. Например, такими пререквизитами могут являться

обновления операционной системы.

Если этот параметр выключен, необходимо установить пререквизиты вручную.

По умолчанию параметр выключен.

- **Разрешать установку новой версии приложения при обновлении**

  Если этот параметр включен, обновления можно устанавливать, только если это приведет к установке новой версии приложения.

  Если этот параметр выключен, приложение не обновляется. Можно позднее установить новые версии приложений вручную или с помощью другой задачи. Например, можно использовать этот параметр, если инфраструктура вашей компании не поддерживает новую версию приложения или если требуется проверить обновление в тестовой инфраструктуре.

  По умолчанию параметр включен.

После установки новой версии приложения может быть нарушена работа других приложений, установленных на клиентских устройствах и зависящих от работы обновляемой приложения.

- **Загружать обновления на устройство, не устанавливая их**

  Если флажок установлен, приложение загружает обновления на устройство, но не устанавливает их автоматически. Затем вы можете вручную установить загруженные обновления.

  Обновления Microsoft загружаются в служебную папку Windows. Обновления сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft) загружаются в папку, указанную в поле **Загрузить обновления для**.

  Если этот параметр выключен, обновления автоматически устанавливаются на устройство.

  По умолчанию параметр выключен.

- **Загрузить обновления для**

Эта папка используется для загрузки обновлений сторонних приложений (приложений, выпущенных производителями, отличными от "Лаборатории Касперского" и Microsoft).

- **Включить расширенную диагностику**

  Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле **Максимальный размер файлов расширенной диагностики, МБ**. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp. Доступ к файлам можно получить с помощью утилиты удаленной диагностики, с помощью нее можно также загрузить или удалить файлы.

  Если эта функция отключена, Агент администрирования записывает трассировку в соответствии с параметрами утилиты удаленной диагностики Kaspersky Security Center. Дополнительная трассировка не записывается.

При создании задачи нет необходимости включать расширенную диагностику. В дальнейшем вам может потребоваться использовать эту функцию, например, если на каком-либо устройстве запуск задачи завершился с ошибкой и вам нужно получить дополнительную информацию во время следующего запуска задачи.

По умолчанию параметр выключен.

- **Максимальный размер файлов расширенной диагностики, МБ**

По умолчанию указано значение 100 МБ и допустимые значения от 1 до 2048 МБ. Специалисты Службы технической поддержки "Лаборатории Касперского" могут попросить вас изменить заданное по умолчанию значение, если в отправленных вами файлах расширенной диагностики недостаточно информации для устранения проблемы.

Перейдите к следующему шагу мастера.

1. Укажите параметры перезагрузки операционной системы:

   - **Не перезагружать устройство**

     Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

   - **Перезагрузить устройство**

     В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

   - **Спросить у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать наиболее удобное время для перезагрузки.

     По умолчанию выбран этот вариант.

   - **Повторять запрос каждые (мин)**

     Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

     По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

     Если параметр выключен, предложение перезагрузки отображается только один раз.

   - **Принудительно перезагрузить через (мин)**

     После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного

времени.

По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Время ожидания перед принудительным закрытием приложения в заблокированных сессиях через (мин)**

  Принудительное завершение работы приложений, когда устройство пользователя заблокировано (автоматически после периода неактивности или вручную).

  Если параметр включен, работа приложений на заблокированном устройстве принудительно прекращается по истечении времени, указанного в поле ввода.

  Если параметр выключен, работа приложений на заблокированном устройстве не прекращается.

  По умолчанию параметр выключен.

2. Если на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, 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.

3. Нажмите на кнопку **Готово**.

   В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо (см. стр. 456).

   > Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

   Задача будет создана, настроена и отобразится в списке задач.

4. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

   Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

   Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. стр. 456).

После выполнения задачи требуемые обновления установлены и уязвимости закрыты.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Об обновлениях приложений сторонних производителей 672

kaspersky

Добавление правил для установки обновлений

Этот параметр доступен при наличии лицензии на Системное администрирование (см. стр. 370).

При установке обновлений программного обеспечения или закрытии уязвимостей в приложениях с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* необходимо указать правила установки обновлений. Эти правила определяют обновления для установки и уязвимости к закрытию.

Точные параметры зависят от того, добавляете ли вы правило для всех обновлений Центра обновления Windows или для обновлений приложений сторонних производителей (то есть приложений производства не "Лаборатории Касперского" и не Microsoft). При добавлении правила для обновления Центра обновления Windows или обновления приложений сторонних производителей вы можете выбрать приложения и версии приложений, для которых вы хотите установить обновления. При добавлении правила для всех обновлений вы можете выбрать обновления, которые необходимо установить, и уязвимости, которые вы хотите закрыть с помощью установки обновлений.

Вы можете добавить правило для установки обновлений следующими способами:

- Добавить правило при создании задачи *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689).
- Добавить правило на вкладке **Параметры приложения** в окне свойств существующей задачи *Установка требуемых обновлений и закрытие уязвимостей*.
- Запустите мастер установки обновлений (см. стр. 675) или мастер закрытия уязвимостей (см. стр. 704).

Добавление правил для всех обновлений

► Чтобы добавить правило для всех обновлений:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. На шаге мастера **Выбор типа правила** выберите **Правило для всех обновлений**.
3. На шаге мастера **Общие критерии** укажите следующие параметры:
   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на

тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

1. Выбор обновлений для установки:

   - **Устанавливать все подходящие обновления**

В этом случае будут установлены все обновления программного обеспечения, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

   - **Устанавливать только обновления из списка**

     В этом случае будут установлены обновления только того программного обеспечения, которые вы выбираете вручную в списке. Этот список содержит все доступные обновления программного обеспечения.

     Например, вы можете задать обновления в следующих случаях: чтобы проверить установку обновлений в тестовом окружении, чтобы обновить только критически важные приложения или чтобы обновить только требуемые приложения.

   - **Автоматически устанавливать все предыдущие обновления приложений, необходимые для установки выбранных обновлений**

     Включите этот параметр, если вы согласны с установкой промежуточных версий приложений, когда это необходимо, для установки выбранных обновлений.

     Если этот параметр выключен, устанавливаются только выбранные версии приложений. Выключите этот параметр, если вы хотите непосредственно обновить приложения, не пытаясь последовательно установить версии приложений. Если установка выбранных обновлений невозможна без установки предыдущих версий приложения, обновление приложения завершается с ошибкой.

     Например, у вас на устройстве установлена версия 3 приложения, вы хотите обновить ее до версии 5, но версия 5 может быть установлена только поверх версии 4. Если этот параметр включен, сначала будет установлена версия 4 программного обеспечения, потом версия 5. Если этот параметр выключен, установить обновление программного обеспечения не удастся.

     По умолчанию параметр включен.

   Перейдите к следующему шагу мастера.

1. Выберите уязвимости, которые будут закрыты с установкой указанного обновления:

- **Закрывать все уязвимости, соответствующие остальным критериям**

В этом случае будут закрыты все уязвимости в приложениях, соответствующие критериям, указанным на шаге мастера **Общие критерии**. Выбрано по умолчанию.

- **Закрывать только уязвимости из списка**

  Закрывать только уязвимости, которые выбраны вручную в списке. Этот список содержит все обнаруженные уязвимости.

  Например, вы можете задать уязвимости в следующих случаях: чтобы проверить закрытие уязвимостей в тестовом окружении, чтобы закрыть уязвимости только в критически важных приложениях или чтобы закрыть уязвимости только в требуемых приложениях.

Перейдите к следующему шагу мастера.

1. Укажите название правила, которое вы добавляете. Вы можете изменить имя правила позже, на вкладке **Параметры приложения**, в окне свойств созданной задачи.

Правило будет создано, настроено и отобразится в таблице правил мастера создания задачи.

Добавление правил для обновлений Центра обновления Windows

► Чтобы добавить правило для обновлений Центра обновления Windows:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.

2. Выберите **Правило для обновлений Windows Update**.

   Перейдите к следующему шагу мастера.

3. На шаге мастера **Общие критерии** укажите следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

   - **Закрывать уязвимости с уровнем критичности, равным или выше**

     Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

     Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или

Предельный). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

- **Закрывать уязвимости с уровнем критичности по MSRC, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный Microsoft Security Response Center (MSRC), равен или превышает значение, выбранное в списке (**Низкий**, **Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

1. В окне **приложения** выберите приложения и версии приложений, для которых вы хотите установить обновления. По умолчанию выбраны все приложения.
2. В окне **Категории обновлений** выберите категории обновлений для установки. Эти категории такие же, как и в каталоге Центра обновления Microsoft. По умолчанию выбраны все категории.
3. В окне **Имя** укажите название добавляемого правила. Вы можете изменить имя правила позже, в разделе **Параметры**, в окне свойств созданной задачи.

После того как мастер создания правил завершит свою работу, правило добавится и отобразится в списке правил мастера создания задачи или в свойствах задачи.

Добавление правил обновления приложений сторонних производителей

► Чтобы добавить правило для обновления приложений сторонних производителей:

1. Нажмите на кнопку **Добавить**.

   Будет запущен мастер создания правила. Для продолжения работы мастера нажмите на кнопку **Далее**.
2. На шаге мастера **Выбор типа правила** выберите **Правило для обновлений сторонних производителей**.
3. На шаге мастера **Общие критерии** укажите следующие параметры:

   - Набор обновлений для установки

     Выберите обновления, которые должны быть установлены на клиентские устройства:

     - **Устанавливать только утвержденные обновления**. В этом случае устанавливаются только одобренные обновления.
     - **Устанавливать все обновления, кроме отклоненных**. В этом случае устанавливаются обновления со статусами *Одобрено* или *Не определено*.
     - **Устанавливать все обновления, включая отклоненные**. В этом случае

устанавливаются все обновления, независимо от их статуса одобрения. Выбирайте этот вариант осмотрительно. Например, используйте этот параметр, если вы хотите проверить установку некоторых отклоненных обновлений на тестовой инфраструктуре.

- **Закрывать уязвимости с уровнем критичности, равным или выше**

  Иногда обновления программного обеспечения могут ухудшить работу пользователя с программным обеспечением. В таких случаях вы можете установить только те обновления, которые являются критическими для программного обеспечения, и пропустить другие обновления.

  Если этот параметр включен, обновления закрывают только те уязвимости, для которых уровень критичности, установленный "Лабораторией Касперского", равен или превышает значение, выбранное в списке (**Средний**, **Высокий**, или **Предельный**). Уязвимости с уровнем критичности ниже выбранного значения не закрываются.

  Если этот параметр выключен, обновления закрывают все уязвимости, независимо от их уровня критичности.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

1. Выберите приложения и версии приложений, для которых вы хотите установить обновления.

   По умолчанию выбраны все приложения.

   Перейдите к следующему шагу мастера.

2. Укажите название правила, которое вы добавляете. Вы можете изменить имя правила позже, на вкладке **Параметры приложения**, в окне свойств созданной задачи.

Правило будет создано, настроено и отобразится в таблице правил мастера создания задачи.

См. также:

Сценарий: обновление приложений сторонних производителей 673

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....702

Параметры задачи Установка требуемых обновлений и закрытие уязвимостей, указанные после создания задачи

После создания задачи *Установка требуемых обновлений и закрытие уязвимостей* на вкладке **Параметры приложения** окна свойств задачи вы можете указать следующие параметры:

- В разделе **Проверочная установка**:
  - **Не проверять**. Выберите этот вариант, если вы не хотите выполнять проверочную установку обновлений.
  - **Выполнить проверку на указанных устройствах**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенных устройствах. Нажмите на кнопку **Добавить** и выберите устройства, на которых нужно выполнить проверочную установку обновлений.

- **Выполнить проверку на устройствах в указанной группе**. Выберите этот вариант, если вы хотите проверить установку обновлений на группе устройств. В поле **Задайте тестовую группу** укажите группу устройств, на которых нужно выполнить проверочную установку.
- **Выполнить проверку на указанном проценте устройств**. Выберите этот вариант, если вы хотите проверить установку обновлений на определенном количестве устройств. В поле **Процент тестовых устройств из общего числа устройств** укажите процент устройств, на которых нужно выполнить проверочную установку обновлений.

После выбора любого параметра, кроме **Не проверять**, в поле **Среднее время для принятия решения о продолжении установки (ч)** укажите количество часов, которое должно пройти от тестовой установки обновлений, до начала установки обновлений на все устройства.

- В разделе **Обновления для установки** вы можете просмотреть список обновлений, которые заданы в задаче. Отображаются только обновления, соответствующие параметрам выбранной задачи.

Подробное описание задачи см. в общих параметрах задачи.

Автоматическое обновление приложений сторонних производителей

Некоторые приложения сторонних производителей могут обновляться автоматически. Поставщик приложения определяет, поддерживает ли приложение функцию автоматического обновления. Если приложение стороннего производителя, установленное на управляемом устройстве, поддерживает автоматическое обновление, вы можете указать параметр автоматического обновления в свойствах приложения. После изменения параметра автоматического обновления Агенты администрирования применяют новый параметр на каждом управляемом устройстве, на котором установлено приложение.

Параметр автоматического обновления не зависит от других объектов и возможностей Системного администрирования. Например, этот параметр не зависит от статуса одобрения обновления или задач установки обновления, таких как *Установка требуемых обновлений и закрытие уязвимостей* и *Закрытие уязвимостей*.

► *Чтобы настроить параметр автоматического обновления для приложения стороннего производителя:*

1. В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений**.
2. Нажмите на имя приложения, для которого вы хотите изменить параметр автоматического обновления.

   Чтобы упростить поиск, вы можете отфильтровать список по столбцам **Статус автоматических обновлений** и **Управление автоматическим обновлением**.

   Откроется окно свойств приложения.
3. В разделе **Общие** выберите значение для следующей функции:

   Статус автоматических обновлений.
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка автоматического обновления применяется к выбранному приложению.

kaspersky

См. также:

Сценарий: обновление приложений сторонних производителей 673

Закрытие уязвимостей в приложениях сторонних производителей

В этом разделе описаны возможности Kaspersky Security Center связанные с закрытием уязвимостей в приложениях, установленных на управляемых устройствах.

В этом разделе

Об обнаружении и закрытии уязвимостей в приложениях

Kaspersky Security Center обнаруживает и закрывает уязвимости в приложениях на управляемых устройствах под управлением операционных систем Microsoft Windows. Уязвимости обнаруживаются в операционных системах и в приложениях сторонних производителей, включая программное обеспечение Microsoft (см. стр. 650).

Обнаружение уязвимостей в приложениях

Для обнаружения уязвимостей Kaspersky Security Center выполняет поиск известных уязвимостей в приложениях на основе признаков из баз данных об известных уязвимостях. База данных создана и поддерживается специалистами "Лаборатории Касперского" в актуальном состоянии. Она содержит информацию об уязвимостях, такую как описание уязвимостей, дата обнаружения уязвимостей и уровень критичности уязвимостей. Информация об уязвимостях в приложениях приведена на сайте "Лаборатории Касперского" (https://threats.kaspersky.com/ru/).

В Kaspersky Security Center для поиска уязвимостей в приложениях используется задача *Поиск уязвимостей и требуемых обновлений*.

Закрытие уязвимостей в приложениях

Для закрытия уязвимостей в приложениях, Kaspersky Security Center использует обновления программного обеспечения выпущенные поставщиками программного обеспечения. Метаданные обновлений программного обеспечения загружаются в хранилище Сервера администрирования в результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*. Эта задача предназначена для загрузки метаданных обновлений для приложений "Лаборатории Касперского" и приложений сторонних производителей. Эта задача автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Вы также можете создать задачу *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 524).

Обновления программного обеспечения для закрытия уязвимостей могут быть представлены в виде полных дистрибутивов или патчей. Обновления программного обеспечения, которые закрывают уязвимости в приложениях, называются *исправлениями*. *Рекомендуемые исправления* это исправления, которые рекомендуются к установке специалистами "Лаборатории Касперского". *Пользовательские исправления* это исправления, которые вручную указываются для установки пользователями. Чтобы установить пользовательское исправление, необходимо создать инсталляционный пакет, содержащий это исправление.

Если лицензия Kaspersky Security Center предусматривает возможности Системного администрирования, используйте задачу *Установка требуемых обновлений и закрытие уязвимостей*. Эта задача автоматически закрывает несколько уязвимостей, устанавливая рекомендуемые исправления. Для этой задачи вы можете вручную настроить определенные правила для закрытия нескольких уязвимостей.

Если лицензия Kaspersky Security Center не предусматривает возможности Системного администрирования, используйте задачу *Закрытие уязвимостей*. С помощью этой задачи можно закрыть уязвимости, установив рекомендуемые исправления для приложений Microsoft и пользовательских исправлений для приложений сторонних производителей.

Из соображений безопасности любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных приложений с помощью технологий "Лаборатории Касперского". Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение.

Специалисты "Лаборатории Касперского" не проводят ручной анализ обновлений приложений сторонних производителей, которые можно установить с помощью Системного администрирования. Также специалисты "Лаборатории Касперского" не занимаются поиском уязвимостей (известных или неизвестных) или недокументированных возможностей в таких обновлениях и не проводят другие виды анализа упомянутых выше обновлений.

> Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.

kaspersky

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей

В этом разделе представлен сценарий обнаружения и закрытия уязвимостей на управляемых устройствах под управлением Windows. Вы можете обнаружить и закрыть уязвимости в операционных системах, в приложениях сторонних производителей, включая приложения Microsoft (см. стр. 650).

Предварительные требования

- Kaspersky Security Center развернут в вашей организации.
- В сети вашей организации есть управляемые устройства под управлением Windows.
- Подключение Сервера администрирования к интернету необходимо для выполнения следующих задач:
  - Составление списка рекомендуемых исправлений уязвимостей в приложениях Microsoft. Список формируется и регулярно обновляется специалистами "Лаборатории Касперского".
  - Закрытие уязвимостей в приложениях сторонних производителей, отличных от приложений Microsoft.

Этапы

Обнаружение и закрытие уязвимостей состоит из следующих этапов:

1. Поиск уязвимостей в программном обеспечении, установленном на управляемых устройствах

   Чтобы найти уязвимости в приложениях, установленных на управляемых устройствах, запустите задачу *Поиск уязвимостей и требуемых обновлений*. После завершения этой задачи, Kaspersky Security Center получает список обнаруженных уязвимостей и требуемых обновлений для приложений сторонних производителей, указанных в свойствах задачи и установленных на устройствах.

   Задача *Поиск уязвимостей и требуемых обновлений* автоматически создается в мастере первоначальной настройки Kaspersky Security Center. Если вы не запускали мастер первоначальной настройки, запустите его сейчас или создайте задачу вручную (см. стр. 682).

   > Вы можете создать задачу *Поиск уязвимостей и требуемых обновлений* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

2. **Просмотр списка обнаруженных уязвимостей в приложениях**

   Просмотрите список **Уязвимости в приложениях** (см. стр. 712) и решите, какие уязвимости нужно закрыть. Чтобы просмотреть подробную информацию о каждой уязвимости, нажмите на имя уязвимости в списке. Для каждой уязвимости в списке вы также можете просмотреть статистику уязвимости на управляемых устройствах (см. стр. 713).

3. **Настройка закрытия уязвимостей**

   Обнаружив уязвимости в приложениях, вы можете закрыть их на управляемых устройствах с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689) или задачи *Закрытие уязвимостей* (см. стр. 708).

   Задача *Установка требуемых обновлений и закрытие уязвимостей* используется для обновления и закрытия уязвимостей в приложениях сторонних производителей, в том числе в приложениях Microsoft, установленных на управляемых устройствах. Эта задача позволяет установить несколько обновлений и закрыть несколько уязвимостей в соответствии с определенными правилами. Обратите внимание, что эту задачу можно создать, только если у вас есть лицензия на Системное администрирование. Чтобы устранить уязвимости в приложениях, задача *Установка требуемых обновлений и закрытие уязвимостей* использует рекомендованные обновления приложений.

   Задача *Закрытие уязвимостей* не требует лицензии для Системного администрирования. Чтобы использовать эту задачу, требуется вручную указать пользовательские исправления для закрытия уязвимостей в приложениях сторонних производителей (см. стр. 711), которые указаны в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для приложений сторонних производителей.

   > Вы можете создать задачу *Установка требуемых обновлений и закрытие уязвимостей* и задачу *Закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эти задачи для устройств, работающих под управлением других операционных систем.

   Вы можете запустить мастер закрытия уязвимостей (см. стр. 704), который автоматически создаст одну из этих задач, или вы можете создать одну из этих задач вручную.

   Если вы создали и настроили задачу *Установка требуемых обновлений и закрытие уязвимостей*, уязвимости будут автоматически закрыты на управляемых устройствах. При запуске созданной задачи, задача сопоставляет список доступных обновлений программного обеспечения с правилами, указанными в параметрах задачи. Все обновления программного обеспечения, которые соответствуют критериям в указанных правилах, загружены в хранилище Сервера администрирования и установлены для закрытия уязвимостей в приложениях.

   Если вы создали задачу *Закрытие уязвимостей*, закрываются только уязвимости в приложениях Microsoft.

4. **Задание расписания задачи**

   Запланируйте автоматическое выполнение задачи *Поиск уязвимостей и требуемых обновлений* на периодической основе, чтобы поддерживать актуальность списка уязвимостей. Рекомендуемый период – один раз в неделю.

   Если вы создали задачу *Установка требуемых обновлений и закрытие уязвимостей*, вы можете задать ее запуск с той же периодичностью, что и для задачи *Поиск уязвимостей и требуемых обновлений*, или реже. При задании расписания задачи *Закрытие уязвимостей*, вам нужно выбрать исправления приложений Microsoft или указать пользовательские исправления для приложений сторонних производителей каждый раз перед запуском задачи.

   При задании расписания задач убедитесь, что задача закрытия уязвимостей запускается после завершения *Поиск уязвимостей и требуемых обновлений*.

5. **Игнорирование уязвимостей в приложениях (если требуется)**

   Вы можете игнорировать уязвимость в приложениях (см. стр. 715) на всех управляемых устройствах или только на выбранных управляемых устройствах.

6. **Запуск задачи закрытия уязвимости**

Запустите задачу *Установка требуемых обновлений и закрытия уязвимостей* или *Закрытие уязвимостей*. Когда задача будет завершена, убедитесь, что в списке задач она имеет статус *Завершена успешно*.

7. **Создание отчета о результатах закрытия уязвимостей в приложениях (если требуется)**

   Чтобы просмотреть статистику о закрытых уязвимостях, сформируйте Отчет об уязвимостях (см. стр. 561). В этом отчете отображается информация об уязвимостях в приложениях, которые не закрыты. Он позволяет выявлять и закрывать уязвимости в программном обеспечении сторонних производителей, включая программное обеспечение Microsoft, которое используется в вашей организации.

8. **Проверка настройки обнаружения и закрытия уязвимостей в приложениях сторонних производителей**

   Убедитесь, что вы выполнили следующее:

   - обнаружили и просмотрели список уязвимостей в приложениях на управляемых устройствах;
   - проигнорировали некоторые уязвимости в приложениях, по желанию;
   - настроили задачу закрытия уязвимости;
   - запланировали запуск задач для поиска и закрытия уязвимостей в приложениях так, чтобы они запускались последовательно;
   - проверили, что задача закрытия уязвимостей была запущена.

См. также:

О приложениях сторонних производителей 650

Закрытие уязвимостей в приложениях сторонних производителей

Чтобы найти уязвимости в приложениях сторонних производителей, вы можете создать и запустить задачу *Поиск уязвимостей и требуемых обновлений* (см. стр. 682) и получить список уязвимостей в приложениях. После получения списка уязвимостей в приложениях вы можете закрыть уязвимости на управляемых устройствах с операционными системами Windows.

Вы можете закрыть уязвимости в операционной системе и приложениях сторонних производителей, включая приложения Microsoft, создав и запустив задачу *Закрытие уязвимостей* (см. стр. 708) или задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689).

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

Также вы можете создать задачу для закрытия уязвимостей в приложениях следующими способами:

- Откройте список уязвимостей и укажите, какие уязвимости необходимо закрыть.

  В результате создается задача закрытия уязвимостей в приложениях. Также можно добавить выбранные уязвимости в существующую задачу.

- Запустите мастер закрытия уязвимостей.

  Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование (см. стр. 370).

  Мастер упрощает создание и настройку задачи закрытия уязвимостей, а также исключает создание избыточных задач.

Закрытие уязвимостей в приложениях с помощью списка уязвимостей

► *Чтобы закрыть уязвимости в приложениях с помощью списка уязвимостей:*

1. Откройте список уязвимостей для изменения, выполнив одно из следующих действий:
   - В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.
   - В главном окне приложения перейдите в раздел **Активы (Устройства)** → **Управляемые устройства** → **<имя устройства>** → **Дополнительно** → **Реестр приложений**.
   - В главном окне приложения перейдите в раздел **Операции** → **Приложения сторонних производителей** → **Реестр приложений** → <название приложения> → **Уязвимости**.

   Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.
2. В списке уязвимостей установите флажки рядом с уязвимостями, которые вы хотите закрыть и нажмите на кнопку **Закрыть уязвимость**.

   Если рекомендуемое обновление программного обеспечения для закрытия одной из выбранных уязвимостей отсутствует, отображается информационное сообщение.

   Для закрытия некоторых уязвимостей в приложениях вам нужно принять Лицензионное соглашение для установки приложений, если это требуется. Если вы отклоняете Лицензионное соглашение, уязвимость в приложении не закроется.
3. Выберите один из следующих вариантов:
   - **Новая задача.**

     Запустится мастер создания задачи. Если у вас есть лицензия на Системное администрирование (см. стр. 370), по умолчанию выбирается тип задачи *Установка требуемых обновлений и закрытие уязвимостей*. Если у вас нет лицензии, по умолчанию выбирается тип задачи *Закрытие уязвимостей*. Следуйте далее указаниям мастера, чтобы завершить создание задачи.
   - **Закрыть уязвимость (добавить правило в указанную задачу).**

     Выберите задачу, в которую вы хотите добавить выбранные уязвимости. Если у вас есть лицензия на Системное администрирование (см. стр. 370), выберите задачу *Установка требуемых обновлений и закрытие уязвимостей*. В выбранную задачу будет автоматически добавлено новое правило для закрытия выбранных уязвимостей. Если у вас нет лицензии, по умолчанию выбран тип задачи *Закрытие уязвимостей*. Выбранные уязвимости добавлены в свойства задачи.

     Откроется окно свойств задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Если вы выбрали создание задачи, она создается и отображается в списке задач, в разделе **Активы (Устройства)** → **Задачи**. Если вы выбрали добавление уязвимостей в существующую задачу, уязвимости сохраняются в свойствах задачи.

Чтобы закрыть уязвимости в приложениях сторонних производителей, запустите задачу *Установка требуемых обновлений и закрытие уязвимостей* или задачу *Закрытие уязвимостей*. Если вы создали задачу *Закрытие уязвимостей*, вам нужно вручную указать обновления программного обеспечения, перечисленных в свойствах задачи.

Закрытие уязвимостей в приложениях с помощью мастера закрытия уязвимостей

Мастер закрытия уязвимости доступен при наличии лицензии на Системное администрирование (см. стр. 370).

► *Чтобы закрыть уязвимости в приложениях с помощью мастера закрытия уязвимостей:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Откроется таблица со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. Установите флажок напротив уязвимости, которую требуется закрыть.
3. Нажмите на кнопку **Запустить мастер закрытия уязвимости**.

   Кнопка недоступна, если вы выбрали более одной уязвимости.

   Откроется мастер закрытия уязвимости. Отобразится список существующих задач. В списке могут присутствовать следующие типы задач:

   - *Установка требуемых обновлений и закрытия уязвимостей.*
   - *Закрытие уязвимостей.*

   Вы не можете изменить задачу *Закрытие уязвимостей* чтобы установить новые обновлений. Для установки новых обновлений можно использовать только задачу *Установка требуемых обновлений и закрытие уязвимостей*.

4. Если вы хотите, чтобы мастер отображал только те задачи, которые закрывают выбранную уязвимость, включите параметр **Показывать только задачи, закрывающие выбранную уязвимость**.
5. Выполните одно из следующих действий:

   - Чтобы запустить задачу, установите флажок рядом с именем задачи и нажмите на кнопку **Запустить**.

     Никаких дальнейших действий не требуется. Вы можете закрыть мастер. Задача выполняется в фоновом режиме.

   - Чтобы добавить правило в существующую задачу *Установка требуемых обновлений и закрытие уязвимостей*:

     a. Установите флажок рядом с добавленной учетной записью и нажмите на кнопку **Добавить правило**.

> Кнопка **Добавить правило** недоступна, если вы выбрали более одной задачи.

Вы не можете добавить правило для задачи *Закрытие уязвимостей*. Если вы выбрали задачу *Закрытие уязвимостей*, появится следующее уведомление: "Для установки обновлений используйте задачу "Установка требуемых обновлений и закрытие уязвимостей"".

b. На открывшейся странице настройте новое правило:

- **Правило для закрытия уязвимостей этого уровня критичности.**
- **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости**

Это правило отображается только для уязвимостей в приложениях Microsoft.

- **Правило закрытия уязвимостей в приложениях от выбранного поставщика**

Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия уязвимости во всех версиях выбранного приложения**

Это правило отображается только для уязвимостей сторонних приложений.

- **Правило для закрытия выбранной уязвимости**
- **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

a. Нажмите на кнопку **Добавить**.

Откроется окно свойств задачи. Новое правило уже добавлено в свойства задачи. Вы можете просмотреть или изменить правило, а также другие параметры задачи. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

- Чтобы создать задачу:

a. Нажмите на кнопку **Новая задача**.

b. На открывшейся странице настройте новое правило:

- **Правило для закрытия уязвимостей этого уровня критичности**
- **Правило для закрытия уязвимостей с помощью обновлений того же типа, что и обновление, определенное в соответствии с рекомендациями для выбранной уязвимости**

Это правило отображается только для уязвимостей в приложениях Microsoft.

- **Правило закрытия уязвимостей в приложениях от выбранного поставщика**

Это правило отображается только для уязвимостей сторонних приложений.

- **Правило закрытия уязвимости во всех версиях выбранного приложения**

Это правило отображается только для уязвимостей сторонних приложений.

- **Правило для закрытия выбранной уязвимости**

- **Одобрить обновления, закрывающие выбранную уязвимость**

Выбранное обновление будет одобрено к установке. Этот параметр доступен, если некоторые примененные правила установки обновления позволяют установку только одобренных обновлений.

По умолчанию параметр выключен.

a. Нажмите на кнопку **Добавить**.

b. Продолжите создавать задачу в мастере создания задачи (см. стр. 689).

Новое правило, добавленное в мастер закрытия уязвимости, отображается на шаге мастера **Задайте правила установки обновлений**. После завершения работы мастера, задача *Установка требуемых обновлений и закрытие уязвимостей* добавлена в список задач.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Создание задачи Закрытие уязвимостей

Задача *Закрытие уязвимостей* позволяет закрыть уязвимости в приложениях на управляемых устройствах. Вы можете закрыть уязвимости в приложениях сторонних производителей, включая приложения Microsoft.

Вы можете создать задачу *Закрытие уязвимостей* только для устройств под управлением Windows. Вы не можете создать эту задачу для устройств, работающих под управлением других операционных систем.

Вы можете создать задачу *Закрытие уязвимостей*, только если у вас есть лицензия на Системное администрирование (см. стр. 370).

Если у вас есть лицензия на Системное администрирование (см. стр. 370), вы не можете создавать задачи с типом *Закрытие уязвимостей*. Чтобы закрыть новые уязвимости, вы можете добавить их в существующую задачу *Закрытие уязвимостей*. Рекомендуется использовать задачу *Установка требуемых обновлений и закрытие уязвимостей* (см. стр. 689) вместо задачи *Закрытие уязвимостей*. Задача *Установка требуемых обновлений и закрытие уязвимостей* позволяет автоматически устанавливать несколько обновлений и закрывать несколько уязвимостей в соответствии с заданными правилами (см. стр. 694).

Вмешательство пользователя может потребоваться при обновлении приложений сторонних производителей или при закрытии уязвимостей в приложениях сторонних производителей на управляемом устройстве. Например, пользователю может быть предложено закрыть приложение стороннего производителя.

► *Чтобы создать задачу Закрытие уязвимостей:*

1. В главном окне приложения перейдите к вкладке **Активы (Устройства)** → **Задачи**.

Вы также можете создать эту задачу в окне свойств устройства на вкладке **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите Kaspersky Security Center.
4. В списке **Тип задачи** выберите тип задачи **Закрытие уязвимостей**.
5. В поле **Название задачи** укажите название новой задачи.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

6. Выберите устройства, которым будет назначена задача (см. стр. 456).

   Перейдите к следующему шагу мастера.

7. Нажмите на кнопку **Добавить**.

   Откроется список уязвимостей.

8. В списке уязвимостей установите флажки рядом с уязвимостями, которые вы хотите закрыть и нажмите на кнопку **ОК**.

   Для уязвимостей в приложениях Microsoft обычно существуют рекомендуемые исправления. Дополнительные действия для них не требуются.

   Для уязвимостей в приложениях сторонних производителей сначала необходимо указать исправление пользователя для каждой уязвимости, которую вы хотите закрыть (см. стр. 711). После этого вы сможете добавить эти уязвимости в задачу *Закрытие уязвимостей*.

   Перейдите к следующему шагу мастера.

9. 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).

   - **Спросить у пользователя**

     На экране клиентского устройства будет выводиться сообщение о том, что устройство должно быть перезагружено вручную. Для этого варианта можно настроить дополнительные параметры: текст сообщения для пользователя, периодичность сообщения, а также время, после которого перезагрузка будет выполнена принудительно (без подтверждения пользователя). Этот вариант является оптимальным для рабочих станций, чтобы пользователи могли выбрать

наиболее удобное время для перезагрузки.

По умолчанию выбран этот вариант.

- **Повторять запрос каждые (мин)**

  Если выбран этот вариант, приложение с определенной частотой предлагает пользователю выполнить перезагрузку операционной системы.

  По умолчанию параметр включен. По умолчанию интервал составляет 5 минут. Допустимые значения: от 1 до 1440 минут.

  Если параметр выключен, предложение перезагрузки отображается только один раз.

- **Принудительно перезагрузить через (мин)**

  После предложения пользователю перезагрузить операционную систему, приложение выполняет принудительную перезагрузку по истечении указанного времени.

  По умолчанию параметр включен. По умолчанию интервал времени составляет 30 минут. Допустимые значения: от 1 до 1440 минут.

- **Принудительно закрывать приложения в заблокированных сеансах**

  Запущенные приложения могут не позволить перезагрузить клиентское устройство. Например, если выполняется работа с документом в текстовом редакторе и изменения не сохранены, приложение не позволяет перезагрузить устройство.

  Если этот параметр включен, такие приложения 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 приложения, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

По умолчанию параметр выключен.

Перейдите к следующему шагу мастера.

1. Задайте параметры учетной записи:

   - **Учетная запись по умолчанию**

     Задача будет запускаться под той же учетной записью, под которой было установлено и запущено приложение, выполняющее 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.

2. Если на шаге **Завершение создания задачи** включить параметр **Открыть окно свойств задачи после ее создания**, 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.

3. Нажмите на кнопку **Готово**.

   В результате работы мастера задача создана. Если включен параметр **Открыть окно свойств задачи после ее создания**, автоматически откроется окно параметров задачи. В этом окне вы можете указать общие параметры задачи и изменить параметры, указанные при создании задачи, если это необходимо (см. стр. 456).

   > Вы также можете открыть окно свойств задачи, нажав на название созданной задачи в списке задач.

   Задача будет создана, настроена и отобразится в списке задач, в разделе **Активы (Устройства)** → **Задачи**.

4. Чтобы запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

   Вы также можете создать расписание запуска задачи на вкладке **Расписание** в окне свойств задачи.

   Подробное описание параметров запуска по расписанию см. в общих параметрах задачи (см. стр. 456).

После выполнения задачи выбранные уязвимости закрыты.

Пользовательские исправления для уязвимостей в приложениях сторонних производителей

Чтобы использовать задачу *Закрытие уязвимостей*, необходимо вручную указать обновления программного обеспечения, чтобы закрыть уязвимости в приложениях сторонних производителей, перечисленные в параметрах задачи. Задача *Закрытие уязвимостей* использует рекомендованные исправления приложений Microsoft и пользовательские исправления для других приложений сторонних производителей.

Пользовательские исправления – это обновления программного обеспечения, которые администратор вручную указывает для установки, чтобы закрыть уязвимости.

► *Чтобы выбрать пользовательские исправления для уязвимостей в приложениях сторонних производителей:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Откроется страница со списком уязвимостей в приложениях сторонних производителей, установленных на управляемых устройствах.

2. В списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости, для которой вы хотите указать пользовательское исправление.

   Откроется окно свойств выбранной уязвимости.

3. На левой панели выберите раздел **Пользовательские и другие исправления**.

Отобразится список пользовательских исправлений для выбранной уязвимости в приложениях.

4. Нажмите на кнопку **Добавить**.

   Отобразится список доступных инсталляционных пакетов. Список отобразившихся инсталляционных пакетов соответствует списку в папке **Операции** → **Хранилища** → **Инсталляционные пакеты**.

   Если вы не создали инсталляционный пакет, содержащий пользовательское исправление для закрытия выбранной уязвимости, вы можете создать пакет сейчас, нажав на кнопку **Создать** и запустив мастер создания инсталляционного пакета.

5. Выберите инсталляционный пакет (или пакеты), содержащий пользовательское исправление (или пользовательские исправления) для выбранной уязвимости.
6. Нажмите на кнопку **Сохранить**.

Указаны инсталляционные пакеты, содержащие пользовательские исправления для уязвимости в приложениях. Когда вы запускаете задачу *Закрытие уязвимостей*, инсталляционный пакет устанавливается и уязвимость в приложении закрывается.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Просмотр информации об уязвимостях в приложениях, обнаруженных на всех управляемых устройствах

После проверки программного обеспечения на управляемых устройствах на наличие уязвимостей (см. стр. 682) вы можете просмотреть список обнаруженных уязвимостей в приложениях. Вы также можете сформировать и просмотреть отчет об уязвимостях (см. стр. 561).

► *Чтобы просмотреть список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах,*

В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

Отобразится список уязвимостей в приложениях, обнаруженных на клиентских устройствах.

► *Чтобы настроить список уязвимостей в приложениях,*

Нажмите на значок **Фильтр** () в верхнем правом углу списка уязвимостей в приложениях и выберите нужный фильтр. Вы также можете выбрать один из предустановленных фильтров в раскрывающемся списке **Предустановленные фильтры** над списком уязвимостей в приложениях.

Вы можете получить подробную информацию о любой уязвимости из списка.

► *Чтобы получить информацию об уязвимости в приложениях,*

в списке уязвимостей в приложениях перейдите по ссылке с названием уязвимости.

Откроется окно свойств уязвимости в приложениях.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Просмотр информации об уязвимостях в приложениях, обнаруженных на выбранных управляемых устройствах

Вы можете просмотреть информацию об уязвимостях в приложениях, обнаруженных на выбранном управляемом устройстве под управлением Windows.

► *Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:*

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

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

► *Чтобы просмотреть свойства выбранной уязвимости в приложениях,*

перейдите по ссылке с названием уязвимости в списке уязвимостей в приложениях.

Откроется окно свойств выбранной уязвимости в приложениях.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Просмотр статистики уязвимостей на управляемых устройствах

Вы можете просмотреть статистическую информацию каждой уязвимости в приложениях на управляемых устройствах. Статистика представлена в виде диаграмм. На диаграмме отображается количество устройств со следующими статусами:

- *Игнорируется на: <количество устройств>*. Этот статус присваивается, если в свойствах уязвимости вы вручную установили параметр игнорировать уязвимость.
- *Закрыта на: <количество устройств>*. Этот статус присваивается, если задача закрытия уязвимости успешно завершена.

- *Запланирована к закрытию на: <количество устройств>*. Этот статус присваивается, если вы создали задачу закрытия уязвимостей, но задача пока еще не завершена.
- *Применено исправление на: <количество устройств>*. Этот статус присваивается, если вы вручную выбрали обновление программного обеспечения, чтобы закрыть уязвимость, но это обновление не закрыло уязвимость.
- *Требует закрытия на: <количество устройств>*. Этот статус присваивается, если уязвимость была закрыта только на некоторых управляемых устройствах, а уязвимость требуется закрыть на других управляемых устройствах.

► *Чтобы просмотреть статистику уязвимости на управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Отобразится страница со списком уязвимостей в приложениях, обнаруженных на управляемых устройствах.
2. Установите флажок рядом с требуемой уязвимостью.
3. Нажмите на кнопку **Статистика уязвимостей на устройствах**.

   Кнопка **Статистика уязвимостей на устройствах** недоступна, если вы выбрали более одной уязвимости.

Отобразится диаграмма статусов уязвимости. Нажав на статус, откроется список устройств, на которых уязвимость имеет выбранный статус.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Экспорт списка уязвимостей в приложениях в текстовый файл

Вы можете скачать список отображаемых уязвимостей в файл формата CSV или TXT. Вы можете отправить эти файлы специалисту по безопасности или сохранить их для статистических целей.

► *Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на всех управляемых устройствах, в текстовый файл:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

   По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

   Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.
2. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

► *Чтобы экспортировать список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве:*

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

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с названием устройства, для которого вы хотите просмотреть обнаруженные уязвимости в приложениях.

   Откроется окно свойств выбранного устройства.

3. В окне свойств выбранного устройства выберите вкладку **Дополнительно**.

4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на выбранном управляемом устройстве.

   По умолчанию экспортируются только уязвимости, отображаемые на текущей странице.

   Если вы хотите экспортировать только определенные уязвимости, установите флажки рядом с этими уязвимостями.

5. Нажмите на кнопку **Экспортировать в TXT** или **Экспортировать в CSV**, в зависимости от формата, который вы хотите экспортировать. Если какая-либо из этих кнопок не отображается, нажмите на кнопку с многоточием и выберите нужный вариант в раскрывающемся списке.

На ваше устройство загружается файл со списком уязвимостей в приложениях.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей 702

Игнорирование уязвимостей в приложениях

Вы можете игнорировать уязвимости в приложениях и не закрывать их. Причины для игнорирования уязвимостей в приложениях могут быть, например, следующими:

- Вы не считаете, что уязвимость в приложении является критической для вашей организации.
- Вы понимаете, что закрытие уязвимости в приложениях может повредить данные приложения, для которого требуется закрыть уязвимость.
- Вы уверены, что уязвимость в приложениях не представляет опасности для сети вашей организации, так как вы используете другие меры для защиты управляемых устройств.

Вы можете игнорировать уязвимость в приложениях на всех управляемых устройствах или только на выбранных управляемых устройствах.

► *Чтобы пропустить уязвимость в приложениях на всех управляемых устройствах:*

1. В главном окне приложения перейдите в раздел **Операции** → **Управление патчами** → **Уязвимости в приложениях**.

   Отображается список уязвимостей в приложениях, обнаруженных на управляемых устройствах.

2. В списке уязвимостей в приложениях нажмите на имя уязвимости в приложениях, которую вы хотите пропустить.

   Откроется окно свойств уязвимости в приложениях.

3. На вкладке **Общие** включите параметр **Игнорировать уязвимость**.
4. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

Уязвимость в приложениях пропускается на всех управляемых устройствах.

► *Чтобы пропустить уязвимость в приложениях на выбранных управляемых устройствах:*

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

   Отобразится список управляемых устройств.

2. В списке управляемых устройств перейдите по ссылке с именем устройства, на котором вы хотите пропустить уязвимость в приложениях.

   Откроется окно свойств устройства.

3. В окне свойств устройства выберите раздел **Дополнительно**.
4. На левой панели выберите раздел **Уязвимости в приложениях**.

   Отобразится список уязвимостей в приложениях, обнаруженных на устройстве.

5. В списке уязвимостей в приложениях выберите уязвимость, которую вы хотите пропустить на выбранном устройстве.

   Откроется окно свойств уязвимости в приложениях.

6. В окне свойств уязвимости в приложениях на вкладке **Общие** включите параметр **Игнорировать уязвимость**.
7. Нажмите на кнопку **Сохранить**.

   Окно свойств уязвимости в приложениях закроется.

8. Закройте окно свойств устройства.

Уязвимость в приложениях пропускается на выбранном устройстве.

Пропущенные уязвимости в приложениях не будут закрыты после завершения работы задачи *Закрытие уязвимостей* и задачи *Установка требуемых обновлений и закрытие уязвимостей*. Вы можете исключить пропущенные уязвимости в приложениях из списка уязвимостей с помощью фильтра.

См. также:

Обнаружение и закрытие уязвимостей в приложениях сторонних производителей.....702

kaspersky

Создание инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Kaspersky Security Center Web Console позволяет выполнять удаленную установку приложений сторонних производителей с помощью инсталляционных пакетов. Такие приложения сторонних производителей включены в соответствующую базу данных "Лаборатории Касперского". База данных создается автоматически при первом запуске задачи *Загрузка обновлений в хранилище Сервера администрирования* (см. стр. 524).

Вы можете создать инсталляционный пакет приложения стороннего производителя из базы данных "Лаборатории Касперского" только если у вас есть лицензия на Системное администрирование (см. стр. 370).

► *Чтобы создать инсталляционный пакет для приложения стороннего производителя из базы "Лаборатории Касперского":*

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания инсталляционного пакета. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Выберите параметр **Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета**.

   Этот параметр доступен при наличии лицензии на Системное администрирование (см. стр. 370).

   Перейдите к следующему шагу мастера.
4. Выберите приложение, для которого требуется создать инсталляционный пакет.

   Перейдите к следующему шагу мастера.
5. Выберите нужный язык локализации в раскрывающемся списке и нажмите на кнопку Далее.

   Этот шаг отображается только если приложение предоставляет несколько языков.
6. Если вам будет предложено принять Лицензионное соглашение для установки, на шаге мастера **Лицензионные соглашения и Политики конфиденциальности** выполните следующие действия:
   a. Перейдите по ссылке **Показать**, чтобы прочитать Лицензионное соглашение на веб-сайте поставщика или просмотреть обновления, для которых требуется лицензия.
   b. Установите флажок **Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения**.
   c. Нажмите на кнопку **Принять все**, чтобы принять все Лицензионные соглашения и Политики конфиденциальности, отображаемые в списке.

7. На шаге мастера **Имя нового инсталляционного пакета** в поле **Имя инсталляционного пакета** укажите имя инсталляционного пакета и нажмите на кнопку **Далее**.

   Созданный инсталляционный пакет загружен на Сервер администрирования. Мастер создания инсталляционного пакета отображает сообщение об успешном создании инсталляционного пакета.

8. Нажмите на кнопку **Готово**.

Созданный инсталляционный пакет отображается в списке инсталляционных пакетов. Вы можете выбрать этот пакет при создании или перенастройке задачи *Удаленная установка программы*.

Вы можете создать и перенастроить задачу *Удаленная установка приложения* с помощью инсталляционного пакета приложения стороннего производителя из базы данных "Лаборатории Касперского", только если у вас есть лицензия на Системное администрирование (см. стр. 370).

См. также:

Сценарий: настройка защиты сети.....393

Просмотр и изменение параметров инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Если вы ранее создавали какие-либо инсталляционные пакеты приложений сторонних производителей, перечисленные в базе "Лаборатории Касперского" (см. стр. 717), вы можете просмотреть и изменить параметры этих пакетов (см. стр. 719).

Изменение параметров инсталляционного пакета приложения стороннего производителя из базы "Лаборатории Касперского" доступно только при наличии лицензии на Системное администрирование (см. стр. 370).

► *Чтобы просмотреть и изменить параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского":*

1. В главном окне приложения перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**.
2. В открывшемся списке инсталляционных пакетов нажмите на имя соответствующего пакета.

   Откроется окно свойств.

3. При необходимости измените параметры.
4. Нажмите на кнопку **Сохранить**.

Изменения сохранены.

См. также:

Сценарий: настройка защиты сети 393

Параметры инсталляционного пакета для приложения стороннего производителя из базы "Лаборатории Касперского"

Параметры инсталляционного пакета приложения стороннего производителя сгруппированы на следующих вкладках:

Не все параметры, перечисленные ниже, отображаются по умолчанию. Вы можете добавить нужные столбцы, нажав на кнопку **Фильтр** и выбрав соответствующие имена столбцов из списка.

- Вкладка **Общие**
  - Поле ввода, содержащее название инсталляционного пакета, которое можно изменить вручную.
  - **Приложение**
  - **Версия**
  - **Размер**
  - **Создан**
  - **Путь**
- Вкладка **Последовательность установки**
  - **Устанавливать необходимые общесистемные компоненты (пререквизиты)**
  - Таблица, в которой отображаются свойства обновления и которая содержит следующие графы:
    - **Название**
    - **Описание**
    - **Источник**
    - **Тип**
    - **Категория**
    - **Уровень важности по MSRC**
    - **Уровень важности**
    - **Уровень важности патча**
    - **Статья**
    - **Бюллетень**
    - **Не назначено к установке (новая версия)**

- **Назначено к установке**
- **Устанавливается**
- **Установлено**
- **Сбой**
- **Требуется перезагрузка**
- **Зарегистрировано**
- **Устанавливается интерактивно**
- **Статус одобрения обновления**
- **Ревизия**
- **Идентификатор обновления**
- **Версия приложения**
- **Заменяемое**
- **Заменяющее**
- **Требуется принять условия Лицензионного соглашения**
- **Описание веб-адреса**
- **Семейство приложений**
- **Приложение**
- **Язык локализации**
- **Не назначено к установке (новая версия)**
- **Требует установки пререквизитов**
- **Режим загрузки**
- **Является патчем**
- **Не установлено**
- **Создан**

- Вкладка **Параметры**, на которой отображаются параметры инсталляционного пакета, их названия, описания и значения, которые используются в качестве параметров командной строки во время установки. Если в пакете таких нет параметров, отображается соответствующее сообщение. Вы можете изменить значения этих параметров.
- Вкладка **История ревизий**, на которой отображается версии инсталляционного пакета и которая содержит следующие графы:
  - **Ревизия** – номер версии инсталляционного пакета.
  - **Время** – дата и время изменения параметров инсталляционного пакета.
  - **Пользователь** – имя пользователя, изменившего параметры инсталляционного пакета.
  - **IP-адрес устройства пользователя** – IP-адрес устройства, с которого был изменен объект.
  - **IP-адрес Web Console** – IP-адрес приложения Kaspersky Security Center Web Console, с помощью которого был изменен объект.
  - **Действие** – действия, которые были выполнены с инсталляционным пакетом в этой ревизии.

- **Описание** – описание ревизии изменения параметров инсталляционного пакета.

  По умолчанию описание ревизии не заполнено. Чтобы добавить описание ревизии, выберите нужную ревизию и нажмите на кнопку **Изменить описание**. В открывшемся окне введите текст описания ревизии.

См. также:

Сценарий: настройка защиты сети 393

Закрытие уязвимостей в изолированной сети

В этом разделе описаны действия, которые вы можете предпринять для закрытия уязвимостей в приложениях сторонних производителей на управляемых устройствах, подключенных к Серверам администрирования и не имеющих доступа в интернет.

В этом разделе

Закрытие уязвимостей в приложениях сторонних производителей в изолированной сети

Вы можете устанавливать обновления и закрывать уязвимости приложений сторонних производителей, установленных на управляемых устройствах в изолированной сети. К таким сетям относятся Серверы администрирования и подключенные к ним управляемые устройства, не имеющие доступа в интернет. Для закрытия уязвимостей в такой сети необходим Сервер администрирования, подключенный к интернету. Используя Сервер администрирования с доступом в интернет, вы сможете загружать патчи (необходимые обновления) и передавать их на изолированные Серверы администрирования.

Вы можете загружать обновления приложений сторонних производителей, выпущенные производителями программного обеспечения, но не можете загружать обновления для программного обеспечения Microsoft на изолированных Серверах администрирования с помощью Kaspersky Security Center.

Подробнее о процессе закрытия уязвимостей в изолированной сети, ознакомьтесь с описанием и схемой этого процесса (см. стр. 723).

Предварительные требования

Перед началом сделайте следующее:

1. Выделите одно устройство для подключения к интернету и загрузки исправлений. Это устройство будет считаться Сервером администрирования с доступом в интернет.
2. Установите Kaspersky Security Center (см. стр. 87) версии не ниже 15.1 на следующих устройствах:
   - Выделенное устройство, которое будет выступать в роли Сервера администрирования с доступом в интернет.
   - Изолированные устройства, которые будут выступать в роли изолированных от интернета Серверов администрирования (далее – изолированные Серверы администрирования).
3. Убедитесь, что на каждом Сервере администрирования достаточно места на диске для загрузки и хранения обновлений и исправлений.

Этапы

Установка обновлений и закрытие уязвимостей в приложениях сторонних производителей на управляемых устройствах, относящихся к изолированным Серверам администрирования, состоит из следующих этапов:

1. **Настройка Сервера администрирования с доступом в интернет**

   Подготовьте Сервер администрирования с доступом в интернет (см. стр. 724) для обработки запросов на необходимые обновления стороннего программного обеспечения и для загрузки.

2. **Настройка изолированных Серверов администрирования**

   Подготовьте изолированные Серверы администрирования (см. стр. 725), чтобы они могли регулярно формировать списки необходимых обновлений и обрабатывать патчи, загружаемые Сервером администрирования с доступом в интернет. После настройки изолированные Серверы администрирования больше не пытаются загружать патчи из интернета. Вместо этого они получают обновления через патчи.

3. **Передача патчей и установка обновлений на изолированные Серверы администрирования**

   Когда настройка Серверов администрирования закончена, вы можете переносить списки обновлений и патчи (см. стр. 726) с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Далее обновления из исправлений будут установлены на управляемые устройства с помощью задачи *Установка требуемых обновлений и закрытие уязвимостей*.

Результаты

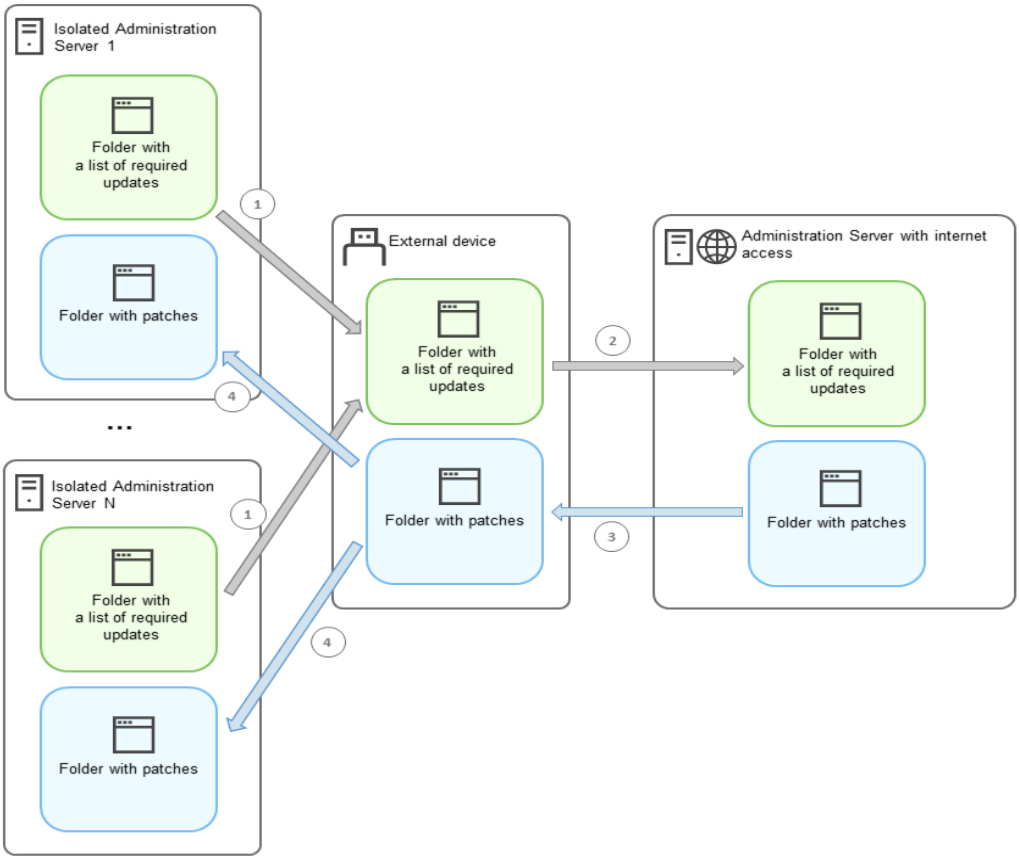
Таким образом обновления программ сторонних производителей передаются на изолированные Серверы администрирования и устанавливаются на подключенные управляемые устройства с помощью Kaspersky Security Center. Достаточно один раз настроить Серверы администрирования, чтобы получать обновления с нужной вам частотой, например, один или несколько раз в день.

См. также:

Выключение передачи патчей и установка обновлений в изолированной сети.....728

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети

Процесс закрытия уязвимостей в приложениях сторонних производителей в изолированной сети показан на рисунке ниже (см. стр. 721). Вы можете периодически повторять этот процесс.



Каждый Сервер администрирования, изолированный от сети интернет (далее — изолированный Сервер администрирования), формирует список обновлений, которые нужно установить на управляемые устройства, подключенные к этому Серверу администрирования. Этот список обновлений хранится в определенной папке в виде набора двоичных файлов, каждый из которых имеет идентификатор патча, содержащего необходимое обновление. Поэтому каждый файл в списке соответствует определенному патчу.

Список требуемых обновлений переносится с изолированного Сервера администрирования на выделенный Сервер администрирования с доступом в интернет с помощью внешнего устройства. После этого назначенный Сервер администрирования загружает патчи из интернета и помещает их в назначенную папку.

Когда все патчи загружены и помещены в указанную папку, они переносятся обратно на каждый изолированный Сервер администрирования, с которого был получен список необходимых обновлений. Патчи сохраняются в специально созданной для них папке на каждом изолированном Сервере администрирования.

В результате задача *Установка требуемых обновлений и закрытие уязвимостей* запускает патчи и устанавливает обновления на управляемые устройства изолированных Серверов администрирования.

См. также:

Закрытие уязвимостей в приложениях сторонних производителей в изолированной сети 721
Передача исправлений и установка обновлений в изолированной сети 726

Настройка Сервера администрирования с доступом в интернет для закрытия уязвимостей в изолированной сети

Чтобы подготовиться к закрытию уязвимостей и передаче патчей в изолированной сети (см. стр. 721), сначала настройте Сервер администрирования с доступом в интернет, а затем настройте изолированные Серверы администрирования (см. стр. 725).

► *Чтобы настроить Сервер администрирования с доступом в интернет:*

1. Создайте две папки на диске (см. стр. 723), где установлен Сервер администрирования:
   - папку для списка необходимых обновлений;
   - папку для патчей.

   Вы можете назвать эти папки по своему желанию.
2. Предоставьте группе KLAdmins право **Изменение** на созданные папки, используя стандартные средства администрирования операционной системы.
3. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
4. Выполните следующие команды в командной строке:
   - Чтобы указать путь к папке для исправлений:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<path to the folder>"
   ```

   - Чтобы задать путь к папке для списка необходимых обновлений:

   ```
   klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<path to the folder>"
   ```

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/FolderForPatches"`
5. При необходимости с помощью утилиты klscflag укажите, как часто Сервер администрирования должен проверять наличие новых запросов на исправления:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <value in seconds>
   ```

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Перезапустите службу Сервера администрирования.

Сервер администрирования с доступом в интернет готов к загрузке и передаче обновлений на изолированные Серверы администрирования. Прежде чем приступить к закрытию уязвимостей, настройте изолированные Серверы администрирования (см. стр. 725).

См. также:

Настройка изолированных Серверов администрирования для закрытия уязвимостей в изолированной сети

После настройки Сервера администрирования с доступом в интернет (см. стр. 724), подготовьте каждый изолированный Сервер администрирования в вашей сети, чтобы закрывать уязвимости и устанавливать обновления (см. стр. 721) на управляемых устройствах, подключенных к этим изолированным Серверам администрирования.

► *Чтобы настроить изолированные Серверы администрирования, выполните следующие действия для каждого Сервера администрирования:*

1. Активируйте лицензионный ключ для Системного администрирования.
2. Создайте две папки на диске (см. стр. 723), где установлен Сервер администрирования:
   - папку для списка необходимых обновлений;
   - папку для патчей.

   Вы можете назвать эти папки по своему желанию.
3. Предоставьте группе KLAdmins право **Изменение** на созданные папки, используя стандартные средства администрирования операционной системы.
4. С помощью утилиты klscflag укажите пути к папкам в свойствах Сервера администрирования.

   Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
5. Выполните следующие команды в командной строке:
   - Чтобы указать путь к папке для исправлений:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<путь к папке>"
```

   - Чтобы задать путь к папке для списка необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<path to the folder>"
```

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`

6. При необходимости с помощью утилиты klscflag укажите, как часто изолированный Сервер администрирования должен проверять наличие новых патчей:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <value in seconds>
   ```

   По умолчанию указано значение 120 секунд.

   Пример: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`

7. При необходимости с используйте утилиту klscflag для вычисления хешей SHA256 патчей:

   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```

   Выполнив эту команду, вы можете убедиться, что патчи не были изменены при их переносе на изолированный Сервер администрирования и что вы получили корректные патчи, содержащие необходимые обновления.

   По умолчанию Kaspersky Security Center не вычисляет хеши SHA256 патчей. Если включить этот параметр, после получения патчей изолированным Сервером администрирования Kaspersky Security Center вычисляет их хеши и сравнивает полученные значения с хешами, хранящимися в базе данных Сервера администрирования. Если вычисленный хеш не совпадает с хешем в базе данных, возникает ошибка и вам необходимо заменить неверные патчи.

8. Создайте (см. стр. 682) задачу *Поиск уязвимостей* и требуемых обновлений и настройте расписание запуска задачи (см. стр. 682). Запустите задачу вручную, если вы хотите, чтобы она выполнялась раньше, чем указано в расписании задачи.

9. Перезапустите службу Сервера администрирования.

После настройки всех Серверов администрирования вы можете переместить исправления и списки необходимых обновлений (см. стр. 726) и закрыть уязвимости приложений сторонних производителей на управляемых устройствах в изолированной сети.

См. также:

Закрытие уязвимостей в приложениях сторонних производителей в изолированной сети 721

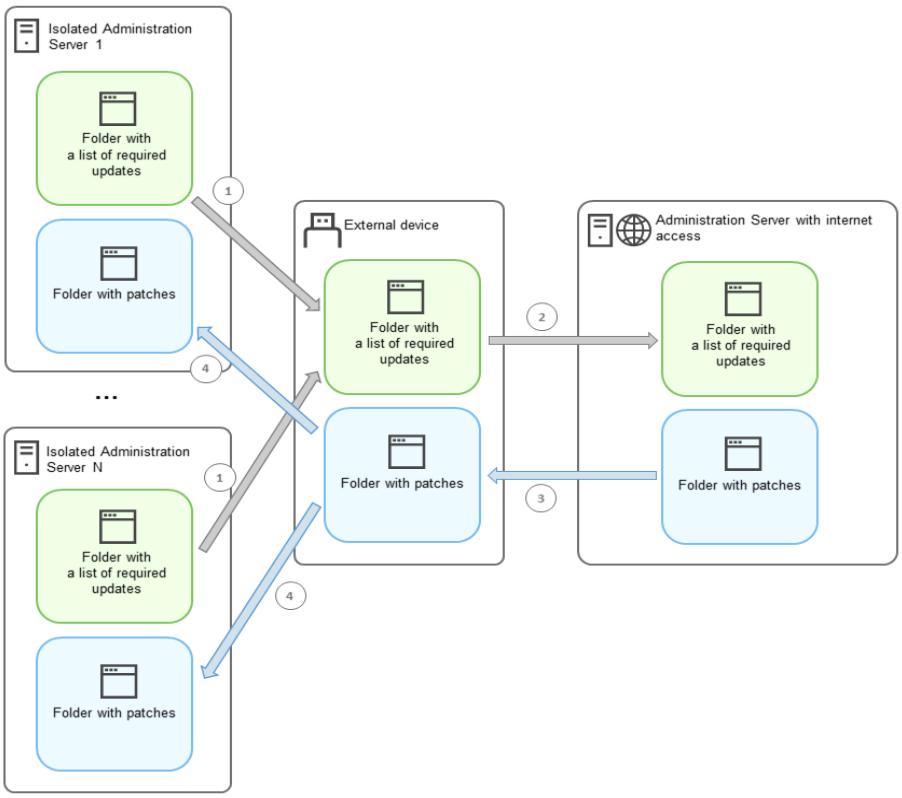
О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети 723

Передача исправлений и установка обновлений в изолированной сети

После того, как настройка Серверов администрирования закончена (см. стр. 721), вы можете переносить патчи с необходимыми обновлениями с Сервера администрирования, имеющего доступ интернет, на изолированные Серверы администрирования. Вы можете передавать и устанавливать обновления с нужной вам частотой, например, один или несколько раз в день.

Съемный диск, например, внешний диск, необходим, для переноса патчей и списка необходимых обновлений между Серверами администрирования. Убедитесь, что внешний диск имеет достаточно места для загрузки и хранения патчей.

Процесс передачи патчей и списка необходимых обновлений показан на рисунке ниже.



► *Чтобы установить обновления и закрыть уязвимости на управляемых устройствах, подключенных к изолированным Серверам администрирования:*

1. Запустите задачу *Установка требуемых обновлений и закрытие уязвимостей*, если она еще не запущена.
2. Подключите внешний диск к любому изолированному Серверу администрирования.
3. Создайте на внешнем диске две папки: одну для списка необходимых обновлений и одну для патчей. Вы можете назвать эти папки по своему желанию.

   Если вы создали эти папки ранее, очистите их.
4. Скопируйте список необходимых обновлений с каждого изолированного Сервера администрирования и вставьте этот список в папку для списка необходимых обновлений на внешнем диске.

   В результате вы объединяете все списки, полученные со всех изолированных Серверов администрирования, в одну папку. В этой папке должны находиться бинарные файлы с идентификаторами патчей, необходимых для всех изолированных Серверов администрирования (см. стр. 723).
5. Подключите внешний диск к Серверу администрирования с доступом в интернет.
6. Скопируйте список необходимых обновлений с внешнего диска и вставьте этот список в папку для списка необходимых обновлений на Сервере администрирования с доступом в интернет.

   Все необходимые патчи автоматически загружаются из интернета в папку патчей на Сервере администрирования. Это может занять несколько часов.

7. Убедитесь, что все необходимые патчей загружены. Для этого можно выполнить одно из следующих действий:
   - Проверьте папку на наличие патчей на Сервере администрирования с доступом в интернет. Все исправления, которые были указаны в списке необходимых обновлений, должны быть загружены в нужную папку. Это удобнее, если требуется небольшое количество исправлений.
   - Подготовьте специальный скрипт, например, shell-скрипт. Если вы получите большое количество патчи, то будет сложно самостоятельно проверить, что все исправления загружены. В таких случаях лучше автоматизировать проверку.
8. Скопируйте патчи с Сервера администрирования с доступом в интернет и вставьте их в соответствующую папку на внешнем диске.
9. Перенесите исправления на каждый изолированный Сервер администрирования. Поместите патчи в специальную папку для них.

В результате каждый изолированный Сервер администрирования формирует актуальный список обновлений, необходимых для управляемых устройств, подключенных к текущему Серверу администрирования. После получения списка необходимых обновлений Сервер администрирования загружает из интернета патчи. При появлении этих патчей на изолированных Серверах администрирования задача *Установка требуемых обновлений и закрытие уязвимостей* обрабатывает патчи. Таким образом, на управляемые устройства устанавливаются обновления и закрываются уязвимости в приложениях сторонних производителей.

При выполнении задачи *Установка требуемых обновлений и закрытие уязвимостей* не перезагружайте устройство Сервера администрирования и не запускайте задачу *Резервное копирование данных Сервера администрирования* (это также вызовет перезагрузку). В результате задача *Установка требуемых обновлений и закрытие уязвимостей* прерывается, а обновления не устанавливаются. В этом случае вам необходимо перезапустить эту задачу вручную или дождаться запуска задачи по настроенному расписанию.

См. также:

Закрытие уязвимостей в приложениях сторонних производителей в изолированной сети 721

О закрытии уязвимостей в приложениях сторонних производителей в изолированной сети 723

Выключение передачи патчей и установка обновлений в изолированной сети

Вы можете выключить передачу исправлений на изолированные Сервера администрирования, например, если вы решили вывести один или несколько Серверов администрирования из изолированной сети (см. стр. 726). Таким образом вы сможете уменьшить количество исправлений и время на их загрузку.

► *Чтобы выключить передачу исправлений на изолированные Серверы администрирования:*

1. Если вы хотите вывести из изоляции все Серверы администрирования, в свойствах Сервера администрирования с доступом в интернет удалите пути к предполагаемым папкам для патчей и

список необходимых обновлений. Если вы хотите, чтобы выбранные Серверы администрирования находились в изолированной сети, пропустите этот шаг.

Запустите командную строку и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag находится в директории, в которой установлен Сервер администрирования. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.

Выполните следующие команды в командной строке:

- Чтобы удалить путь к папке с патчами:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
```

- Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
```

2. Перезапустите службу Сервера администрирования с доступом в интернет, если вы удалили пути к папкам.
3. В свойствах каждого изолированного Сервера администрирования, который вы хотите вывести из изоляции, удалите пути к папкам для патчей и список необходимых обновлений.

   Выполните следующие команды в командной строке под учетной записью с правами root:

   - Чтобы удалить путь к папке с патчами:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
```

   - Чтобы удалить путь к папке со списком необходимых обновлений:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
```

4. Перезапустите службу каждого Сервера администрирования, на котором вы удалили пути к папкам.

Если вы перенастроили Сервер администрирования с выходом в интернет, патчи больше не будут передаваться через Kaspersky Security Center.

Если вы перенастроили только определенные Серверы администрирования и удалили их из изолированной сети, они больше не будут получать патчи через Kaspersky Security Center. Только те Серверы администрирования, которые остаются в изолированной сети, будут продолжать получать исправления.

Если вы хотите в будущем приступить к закрытию уязвимостей на отключенных изолированных Серверах администрирования, вам необходимо настроить эти Серверы администрирования и Сервер администрирования с доступом в интернет еще раз (см. стр. 721).

См. также:

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 клиентское приложение.

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/15.1/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. 51), запускать задачи (см. стр. 58) в Kaspersky Security Center или назначать точки распространения (см. стр. 61). Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

► *Чтобы вызвать методы OpenAPI и запустить сценарии:*

1. Загрузите архив https://support.kaspersky.com/help/KSC/15.1/KSCAPI/common/KlAkOAPI-15.1.tar.gz. Этот архив включает в себя пакет KlAkOAPI и примеры (их можно скопировать из архива или справочного руководства по OpenAPI). Также архив KlAkOAPI.tar.gz находится в папке установки Kaspersky Security Center.
2. Установите пакет KlAkOAPI из архива KlAkOAPI.tar.gz на устройстве, на котором установлен Сервер администрирования https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00453.html.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

Таблица 52. Сопоставление пользовательских сценариев и примеров методов Kaspersky Security Center OpenAPI

Пример	Назначение примера	Сценарий
Журнал событий Log KlAkParams https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00436.html	Вы можете извлекать и обрабатывать данные, используя `KlAkParams` структуру данных. 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 (см. стр. 544)

Пример	Назначение примера	Сценарий
Создание и удаление первичного/вторичного отношения https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00437.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. 177) и удаление иерархии Серверов администрирования (см. стр. 194).
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00440.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 63), а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений (см. стр. 285)
Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00441.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 приложений (см. стр. 379)
Создайте отчет об эффективных правах пользователей https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00442.html	Вы можете создать разные отчеты https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00032.html. Например, вы можете сгенерировать отчет об эффективных правах пользователя, используя этот пример. В этом отчете представлена информация о правах, которыми обладает пользователь в зависимости от его группы и роли. Вы можете загрузить отчет в формате HTML, PDF или Excel.	Генерация и просмотр отчета (см. стр. 561)
Запустите задачу на устройстве https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00443.html	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения (см. стр. 63), а затем запустить необходимую задачу.	Запустите задачу вручную (см. стр. 455).

Пример	Назначение примера	Сценарий
Регистрация точек распространения для устройств в группе https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00445.html	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и приложений "Лаборатории Касперского" (см. стр. 515)
Перечисление всех групп https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00446.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. 173)
Перечисление задач, запрос статистики задач и запуск задач https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00447.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.	Управление задачами (см. стр. 452)
Создание и запуск задачи https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00448.html	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Название. • 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/15.1/KSCAPI/a00030.html.	Создание задачи (см. стр. 454)

Пример	Назначение примера	Сценарий
Перечисление лицензионных ключей https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00449.html	Вы можете получить список всех активных лицензионных ключей для приложений "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00122.html о каждом лицензионном ключе, такие как имя, тип или срок действия.	Просмотр информации об используемых лицензионных ключах (см. стр. 385)
Создание и поиск внутреннего пользователя https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00450.html	Вы можете создать учетную запись для дальнейшей работы.	Добавление учетной записи внутреннего пользователя (см. стр. 491)
Создание пользовательской категории https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00451.html	Вы можете создать категорию приложений с требуемыми параметрами https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00459.html.	Создание пополняемой вручную категории приложений (см. стр. 659)
Перечисление пользователей с помощью SrvView https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00452.html	Вы можете использовать класс SrvView https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00593.html для запроса подробной информации https://support.kaspersky.com/help/KSC/15.1/KSCAPI/a00159.html с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление пользователями и ролями пользователей (см. стр. 475)

Программы, взаимодействующие с Kaspersky Security Center через OpenAPI

Некоторые программы взаимодействуют с Kaspersky Security Center через OpenAPI. К таким приложениям относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательское клиентское приложение, разработанное 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. 174) для подключения к Серверу администрирования, добавьте IP-адреса устройств, на которых установлены приложения, использующие Kaspersky Security Center OpenAPI. Чтобы узнать, работает ли используемое вами приложение с OpenAPI, обратитесь к справке этого приложения.

kaspersky

Руководство по масштабированию

В этом руководстве представлена информация по масштабированию Kaspersky Security Center https://help.kaspersky.com/KSCLinux/15/ru-RU/162088.htm.

См. также:

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 приложении, 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 приложений (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 приложения "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

Источники информации о приложении

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

На странице Kaspersky Security Center (https://www.kaspersky.ru/small-to-medium-business-security/security-center) вы можете получить общую информацию о приложении, его возможностях и особенностях работы.

Страница Kaspersky Security Center в Базе знаний

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

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

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.

Обсуждение приложений "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем форуме (https://community.kaspersky.com/).

На форуме пользователей вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

> Для отображения справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки (см. стр. 735).

kaspersky

Список ограничений

Kaspersky Security Center имеет ряд ограничений, не критичных для работы приложения:

- При нажатии на имя кластера в списке **Кластеры и массивы серверов** (**Активы (Устройства)** → **Управляемые устройства** → **Кластеры и массивы серверов**) окно свойств кластера не открывается.
- При импорте задачи *Загрузить обновления в хранилища точек распространения* или задачи *Проверка обновлений* параметр **Выбор устройств, которым будет назначена задача** включен. Эти задачи невозможно назначить выборкам устройств или заданным устройствам. Если вы назначите задачу *Загрузить обновления в хранилища точек распространения* или задачу *Проверка обновлений* на определенные устройства, задача будет импортирована некорректно.
- Если в вашей сети есть домен Microsoft Active Directory, содержащий несколько десятков тысяч объектов (управляемые устройства, группы безопасности и учетные записи пользователей), а размер страницы ответа (параметр `MaxPageSize`) меньше 5000, опрос контроллера домена недоступен и информация о доменных объектах не поступает. При попытке опроса контроллера домена возникает ошибка *Превышено предельное значение размера*. Увеличение размера страницы ответа может помочь исправить ошибку. Вы можете использовать утилиту Ntdsutil.exe https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/view-set-ldap-policy-using-ntdsutil, чтобы увеличить значение параметра `MaxPageSize` до `5000` или до `10000`, если необходимо.
- Если вы включаете KPSN в свойствах Сервера администрирования и используете HTTPS-порт 17111, соединение с ds.kaspersky.com не прерывается.
- Kaspersky Endpoint Security для Windows не поддерживает службу прокси-сервера KSN, если в параметрах прокси-сервера KSN свойств Сервера администрирования включен параметр **Использовать HTTPS** и адрес Сервера администрирования содержит нелатинские символы.
- При переходе на подчиненный Сервер из интерфейса главного Сервера администрирования Kaspersky Security Center функциональность обновления через службу обновлений "Лаборатории Касперского" (**Seamless Update - SMU**) недоступна.
- При создании задачи *Добавить ключ* для Kaspersky Endpoint Security 11.3 для Mac мастер отображает таблицу лицензионных ключей, которая может содержать пустые строки.
- Уровень защиты, отображаемый в политике Kaspersky Endpoint Security для Windows, не соответствует уровню защиты в интерфейсе Kaspersky Endpoint Security для Windows.
- При запуске задачи *Удаленная деинсталляция приложения* для удаления Kaspersky Endpoint Security для Linux с управляемого устройства задача завершается успешно, но Kaspersky Endpoint Security для Linux не удаляется. Эта проблема актуальна для Kaspersky Endpoint Security для Linux, Kaspersky Embedded Systems Security for Linux и Kaspersky Industrial CyberSecurity for Linux Nodes.
- В окне свойств Сервера администрирования содержатся параметры для мобильных устройств, однако Kaspersky Security Center не поддерживает управление мобильными устройствами.
- Если на устройстве с операционной системной Linux обнаружено приложение из раздела **Реестр приложений**, в свойствах приложения 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 приложения.

- В отчетах с буквенным форматом разрыв страницы может обрезать строку текста по горизонтали.
- 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.
- 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 невозможно 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.
- При запуске задачи *Удаленное выполнение скриптов* вы не можете изменить учетную запись, которая назначена задаче. Чтобы изменить учетную запись, которой назначена задача, остановите задачу в параметрах задачи и создайте задачу снова с требуемой учетной записью.
- Задача *Изменение пароля учетной записи* может работать некорректно, если на пользовательском устройстве включен SELinux. Дополнительные сведения о выключении SELinux см. в руководстве пользователя для вашей операционной системы.

kaspersky

Глоссарий

А

Активный ключ

Ключ, используемый в текущий момент для работы приложения.

Д

Дополнительный лицензионный ключ

Ключ, подтверждающий право на использование приложения, но не используемый в текущий момент.

К

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.

Г

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждого из установленных в группе приложений могут быть созданы групповые политики и сформированы групповые задачи.

С

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 приложениями.

С

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.

К

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлены Агент администрирования и управляемые приложения "Лаборатории Касперского".

Р

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 приложений, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

А

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Р

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 приложений "Лаборатории Касперского".

kaspersky

А

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.

П

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

М

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.

А

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Д

Доступное обновление

Пакет обновлений модулей приложений "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре приложения.

Х

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

kaspersky

Ш

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).

Ц

Централизованное управление приложением

Удаленное управление приложением при помощи служб администрирования, предоставляемых Kaspersky Security Center.

А

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной защиты организации-клиента.

К

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Ш

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.

Д

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

В

Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

Н

Непосредственное управление приложением

Управление приложением через локальный интерфейс.

Т

Точка распространения

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки приложений, 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.

Х

Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center.

У

Уровень важности события

Характеристика события, зафиксированного в работе приложения "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.

kaspersky

П

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.

Г

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

Д

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.

Н

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.

Н

Несовместимое приложение

Антивирусное приложение стороннего производителя или приложение "Лаборатории Касперского", не поддерживающее управление через Kaspersky Security Center.

И

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки приложения "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки приложения и обеспечения его работоспособности сразу после установки. Значения параметров соответствуют значениям параметров приложения по умолчанию.

Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива приложения.

B

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.

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.

A

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

O

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

K

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.

kaspersky

В

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.

С

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых приложения "Лаборатории Касперского" получают обновления баз и модулей приложений.

Ф

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать приложение "Лаборатории Касперского" по пробной или коммерческой лицензии.

С

Срок действия лицензии

Период, в течение которого вы можете пользоваться функциями приложения и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Г

Группа лицензионных приложений

Группа приложений, созданная на основании заданных администратором критериев (например, по производителю), для которых ведется учет установок на клиентских устройствах.

Л

Локальная установка

Установка приложения безопасности на устройство сети организации, которое предусматривает ручной запуск установки из дистрибутива приложения безопасности или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

Л

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском компьютере.

kaspersky

У

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Р

Ручная установка

Установка приложения безопасности на устройство сети организации из дистрибутива приложения безопасности. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

А

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 приложений, разработанных для систем Microsoft Windows. Для приложений "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.

А

Антивирусная защита 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 приложений безопасности и сервисов, а также при наличии и соблюдении политики информационной безопасности в организации.

С

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных приложений безопасности, использование лицензионных ключей, количество и виды обнаруженных угроз.

П

Политика

Политика определяет параметры работы приложения и доступ к настройке приложения, установленного на устройствах группы администрирования. Для каждого приложения требуется создать свою политику. Вы можете создать множество политик для приложений, установленных на устройствах в каждой группе

администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждому приложению.

П

Профиль

Набор параметров поведения мобильных устройств Exchange при подключении к серверу Microsoft Exchange.

П

Параметры приложения

Параметры работы приложения, общие для всех типов его задач и отвечающие за работу приложения в целом, например: параметры производительности приложения, параметры ведения отчетов, параметры резервного хранилища.

С

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Р

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

У

Удаленная установка

Установка приложений "Лаборатории Касперского" при помощи инструментов, предоставляемых приложением Kaspersky Security Center.

В

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.

kaspersky

В

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 приложений, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов приложений для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Р

Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами (см. стр. 741).

А

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.

О

Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

S

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

З

Задача

Функции, выполняемые приложением "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

З

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

П

Параметры задачи

Параметры работы приложения, специфичные для каждого типа задачи.

О

Обновление

Процедура замены или добавления новых файлов (баз или модулей приложений), получаемых с серверов обновлений "Лаборатории Касперского".

В

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

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center позволяет просматривать результаты выполнения групповых задач, задач для наборов устройств и задач Сервера администрирования. Просмотр результатов выполнения локальных задач недоступен.

► *Чтобы посмотреть результаты выполнения задачи:*

1. В окне свойств задачи выберите раздел **Общие**.
2. По ссылке **Результаты** откройте окно **Результаты выполнения задачи**.

kaspersky

Проверка целостности модулей с помощью утилит klscmodchk и integrity_checker

Приложение 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 приложения другими файлами, содержащими вредоносный код. Чтобы избежать подмены модулей и файлов приложения, в приложении Kaspersky Security Center предусмотрена проверка целостности компонентов приложения с помощью утилит klscmodchk и integrity_checker. Утилиты проверяют модули и файлы на наличие неавторизованных изменений или повреждений. Если модуль или файл приложения 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 приложения. Файл манифеста компонента приложения содержит файлы, целостность которых важна для корректной работы компонента приложения. 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 приложения, выполните любую из следующих команд:*

- `$ klscmodchk`

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

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

  Опции приложения `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 приложения.

kaspersky

Разделение доступа к функциям приложения 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 приложения: 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 приложения, 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 53. 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 приложения	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 приложением; • изменять права доступа пользователей к функциям Kaspersky Security Center.

Обновление антивирусных баз в ручном режиме

Для обновления антивирусных баз, находящихся в изолированном сегменте сети, рекомендуется использовать следующий порядок действий:

1. В приложении 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 приложениями, 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, приложения еще раз проведут контроль целостности загружаемых обновлений.

kaspersky

Устранение уязвимостей и установка критических обновлений в приложении

"Лаборатория Касперского" может выпускать обновления приложения, 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 приложения, 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 приложения, должно периодически (не реже одного раза в три месяца) проверять отсутствие обнаруженных уязвимостей в приложении, 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 приложения следующими способами:

- По адресу электронной почты vulnerability@kaspersky.com.
- В сообществе пользователей "Лаборатории Касперского".

kaspersky

Действия после сбоя или неустранимой ошибки в работе приложения

Приложение автоматически восстанавливает свою работу после сбоев, участие пользователя не требуется. В случае, когда приложение не может восстановить свою работу, вам требуется переустановить приложение или его компонент. Вы также можете обратиться за помощью в Службу технической поддержки (см. стр. 735).

kaspersky

Способы получения технической поддержки

Если вы не нашли решения вашего вопроса в документации Kaspersky Security Center или других источниках информации о приложении, 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 приложений (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 приложения "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

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки приложения.

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 является либо зарегистрированным товарным знаком, либо товарным знаком 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 Jabber, 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.

Radmin – зарегистрированный товарный знак компании Famatech.

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.

Logitech является зарегистрированным товарным знаком или товарным знаком компании Logitech в США и (или) других странах.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, 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.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

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.

Соответствие терминов

В этом разделе приведено соответствие терминов, используемых в документации, и терминов, используемых в требованиях ФСТЭК.

Таблица 54. Соответствие терминов

Термин в документации	Термин в требованиях ФСТЭК
приложение	продукт, объект оценки, программное изделие
виртуальная инфраструктура VMware	среда функционирования
файл виртуальной машины	объект воздействия
вирус, приложение, представляющее угрозу, вредоносное приложение	КВ, компьютерный вирус
антивирусные базы, базы приложения	базы данных признаков компьютерных вирусов (БД ПКВ)
антивирусная проверка	поиск вирусов
события	данные аудита
администратор	администратор безопасности, уполномоченный субъект информационной системы, уполномоченный пользователь

kaspersky

Приложение. Сертифицированное состояние приложения: параметры и их значения

Этот раздел содержит перечень параметров приложения, влияющих на безопасное состояние приложения, 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 приложение из безопасного состояния.

Сертифицированная конфигурация приложения не включает в себя функциональность Kaspersky XDR Expert.

Таблица 55. Параметры и их значения для приложения в сертифицированном состоянии

Параметр	Краткое описание и диапазон значений	Значение параметра для приложения 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 каждого управляемого приложения 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 приложения 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 приложений "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 приложение не передавало 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 приложений к серверам активации "Лаборатории Касперского". Возможные значения: • отключена; • включена.	Отключена.

Параметр	Краткое описание и диапазон значений	Значение параметра для приложения 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 приложения.	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 приложения.	Не меньше 400 000 событий.

Параметр	Краткое описание и диапазон значений	Значение параметра для приложения в сертифицированном состоянии
Срок хранения событий	Срок, в течение которого события хранятся в базе данных Сервера администрирования, необходимый для проведения аудита приложения.	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.
Срок хранения ревизий изменений объектов	Срок, в течение которого хранятся ревизии изменений объектов, необходимый для проведения регулярного аудита приложения.	Не меньше 90 дней.
Объявления "Лаборатории Касперского"	Объявления "Лаборатории Касперского" предоставляют информацию о вашей версии Kaspersky Security Center и управляемых приложениях, 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** приложения 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.

Параметр	Краткое описание и диапазон значений	Значение параметра для приложения в сертифицированном состоянии
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 приложения Kaspersky Security Center. Настройка приложения по эталонным параметрам необходима для работы сертифицированной конфигурации приложения.

Месторасположение папки общего доступа Сервера администрирования

Папка общего доступа не должна находиться в папке установки Сервера администрирования.

► *Чтобы изменить папку общего доступа установленного Сервера администрирования:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На вкладке **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 приложения Агента администрирования и управляемых приложений, таких как Kaspersky Endpoint Security для Linux. Создайте политики, как описано в инструкции (см. стр. 409).

Установка применимых обновлений со статусом одобрения "Не определено"

По умолчанию патчи "Лаборатории Касперского" со статусом одобрения *Не определено* устанавливаются автоматически на управляемые устройства сразу после загрузки с серверов обновлений. Необходимо отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения *Не определено*.

► *Чтобы отключить автоматическую установку патчей "Лаборатории Касперского" со статусом одобрения* Не определено:

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику Агента администрирования.

   Откроется окно свойств политики.
3. В открывшемся окне свойств политики выберите вкладку **Параметры и приложения**.
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:*

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 вкладку **Расписание**.
4. В поле **Запуск по расписанию** выберите значение **Каждый N час**.
5. В поле **Интервал запуска (ч)** установите значение 1.
6. Нажмите на кнопку **Сохранить**.

Автоматический запуск задачи Сервера администрирования **Загрузка обновлений в хранилище Сервера администрирования** один раз в час настроен.

Если в сети организации назначены точки распространения, необходимо также настроить автоматический запуск задачи **Загрузка обновлений в хранилища точек распространения**. Для этого необходимо повторить действия, описанные выше для задачи **Загрузка обновлений в хранилище Сервера администрирования**.

Запуск задачи Установка обновлений

После выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования** необходимо настроить запуск задачи **Установка обновлений**.

► *Чтобы настроить автоматический запуск задачи **Установка обновлений** после выполнения задачи **Загрузка обновлений в хранилище Сервера администрирования**:*

1. В разделе **Устройства** выберите раздел **Задачи**.
2. Выберите задачу **Установка обновлений**.

   В результате откроется окно свойств задачи.
3. В окне свойств выберите вкладку **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:*

1. На вкладке **Устройства** выберите **Задачи**.
2. Выберите задачу **Загрузка обновлений в хранилище Сервера администрирования**.
3. В окне свойств задачи перейдите в раздел **Параметры приложения**.
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:*

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 приложение.
4. Нажмите на кнопку **ОК**.

Сервер администрирования необходимо активировать при помощи файлов ключа, так как при активации приложения с помощью кода активации приложения регулярно отправляет запросы на серверы активации "Лаборатории Касперского" для проверки текущего статуса ключа.

Служба прокси-сервера активации "Лаборатории Касперского"

Необходимо отключить службу прокси-сервера активации "Лаборатории Касперского".

► *Чтобы отключить службу прокси-сервера активации "Лаборатории Касперского":*

1. 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 приложение должно использовать только доверенные каналы. Для этого на устройстве с установленным Сервером администрирования необходимо закрыть не использующие SSL-протоколы порты, по которым происходит соединение с Сервером администрирования извне. По умолчанию используется порт 14000. В политике Агента администрирования необходимо настроить использование SSL-соединения.

► *Чтобы настроить использование SSL-соединения в политике Агента администрирования:*

1. В разделе **Устройства** выберите раздел **Политики и профили политик**.
2. Выберите политику **Агент администрирования**.

   Откроется окно свойств политики.
3. В окне свойств политики перейдите в раздел **Параметры приложения**.
4. Выберите подраздел **Сеть**.
5. В подразделе **Сеть** выберите вложенный раздел **Подключения** и нажмите на кнопку **Параметры**.
6. В окне свойств профиля подключения установите флажок **Использовать SSL-соединение**.

   Флажок **Использовать SSL-соединение** необходимо установить для всех профилей подключений.
7. Нажмите на кнопку **ОК**.

Подключение Агента администрирования к Серверу администрирования будет выполняться через защищенный порт с использованием SSL-протокола.

Права пользователей

Внутренним пользователям Kaspersky Security Center должны быть назначены минимально необходимые права для выполнения их функций в программе. Для этого вы можете назначить пользователю или группе пользователей роль с набором прав на работу с Сервером администрирования.

► *Чтобы назначить роль пользователю или группе пользователей:*

1. В разделе **Пользователи и роли** выберите раздел **Пользователи**.
2. В поле **Полное имя** выберите пользователя или группу пользователей, которым нужно присвоить роль.

   Если пользователь или группа отсутствуют в поле, добавьте их по кнопке **Добавить**.
3. Перейдите на вкладку **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 вкладке **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:*

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. 608).

   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 приложения. Рекомендуется хранить не менее 400 000 событий в базе данных Сервера администрирования.

► *Чтобы изменить максимальное количество событий, хранящихся в базе данных Сервера администрирования:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На вкладке **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, приложение удаляет самые старые события и записывает новые.

Срок хранения событий

Для проведения аудита приложения, необходимо настроить срок хранения событий в базе данных Сервера администрирования.

► *Чтобы изменить срок хранения событий:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. Выберите вкладку **Настройка событий**.
3. Установите время хранения событий по уровню их важности:
   - На вкладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На вкладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На вкладке **Предупреждение** выберите нужное событие и установите необходимое значение (не меньше 90 дней).
   - На вкладке **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:*

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 вкладке **Критическое событие** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На вкладке **Отказ функционирования** выберите нужное событие и установите необходимое значение (не меньше 180 дней).
   - На вкладке **Предупреждение** выберите нужное событие установите необходимое значение (не меньше 90 дней).
   - На вкладке **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 приложения. Рекомендуемый срок хранения ревизий изменения объектов 90 дней. Такой срок достаточен для проведения регулярного аудита приложения.

► *Чтобы изменить срок хранения ревизий изменения объектов:*

1. В верхней части экрана нажмите на значок **Параметры** () рядом с именем требуемого Сервера администрирования.
2. На вкладке **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. 617).

Максимальное количество попыток ввода пароля для подключения пользователя к Kaspersky Security Center

Установите максимальное количество попыток ввода пароля, как описано в инструкции (см. стр. 510). Рекомендуется установить значение не больше 10 попыток.

kaspersky

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.

kaspersky

Предметный указатель

R

А

В

Г

З

И

К

Л

О

П

Т