Содержание

Справка Kaspersky Security Center 14 Linux

Что нового

Узнайте, что нового в этой версии программы.

Замещение программ безопасности сторонних производителей

Узнайте о методах удаления несовместимых программ.

Аппаратные и программные требования

Проверьте поддерживаемые операционные системы и версии программ.

Установка

Установка Сервера администрирования и Kaspersky Security Center 14 Web Console.

Обнаружение устройств в сети

Обнаружение существующих и новых устройств в сети вашей организации.

Программы "Лаборатории Касперского". Централизованное развертывание

Планирование ресурсов: установка Сервера администрирования, установка Агента администрирования и программ безопасности на клиентских устройствах.

Программы "Лаборатории Касперского". Лицензирование и активация

Активация программ "Лаборатории Касперского" в несколько шагов.

Руководство по масштабированию (только онлайн-справка)

Для оптимальной производительности при различных условиях учитывайте количество устройств в сети, топологию сети и необходимый вам набор функций Kaspersky Security Center.

Настройка защиты сети

Управление безопасностью организации.

Программы "Лаборатории Касперского". Обновление баз и программных модулей

Поддержка надежности системы защиты.

Мониторинг и отчеты

Просмотр данных об инфраструктуре вашей сети, статусе защиты и статистики.

Настройка точек распространения и шлюзов соединений

Настройка точек распространения.

Экспорт событий в SIEM-системы

Настройте экспорт событий в SIEM-системы для анализа.

Что нового

Kaspersky Security Center 14 Linux

В программе Kaspersky Security Center 14 Linux реализовано несколько новых функций и улучшений:

- Кроме задачи *Загрузка обновлений в хранилище Сервера администрирования*, антивирусные базы для программ безопасности "Лаборатории Касперского" теперь можно загружать с помощью задачи *Загрузка обновлений в хранилища точек распространения*.
- Антивирусные базы и программные модули на управляемых устройствах могут распространяться и обновляться через Сервер администрирования или точки распространения. Вы можете выбрать схему обновления, оптимальную для вашей организации, чтобы снизить нагрузку на Сервер администрирования и оптимизировать трафик данных в корпоративной сети.
- Kaspersky Security Center загружает с серверов обновлений "Лаборатории Касперского" только те обновления, которые запрашиваются программами безопасности "Лаборатории Касперского". Это уменьшает размер загружаемых данных.
- Теперь вы можете использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули. Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и программных модулей.
- Добавлена задача *Проверка обновлений*. С помощью этой задачи вы можете автоматически проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства.
- Kaspersky Security Center теперь поддерживает Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 как управляемую программу.

О Kaspersky Security Center Linux

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

Kaspersky Security Center Linux (далее так же Kaspersky Security Center) предназначен для развертывания и управления защитой устройств с операционной системой Linux® с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux.

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

По сравнению с Сервером администрирования Kaspersky Security Center на базе Windows®, Kaspersky Security Center Linux имеет другой набор функций.

Программа Kaspersky Security Center Linux 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 защиты, построенной на основе программ "Лаборатории Касперского".
- Выполнять удаленную установку программ "Лаборатории Касперского" и других программ сторонних производителей.
- Централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.
- Получать статистику и отчеты о работе программ и устройств.
- Получать уведомления о критических событиях в работе программ "Лаборатории Касперского".
- Проводить инвентаризацию оборудования, подключенного к сети организации.

Централизованно работать с файлами, помещенными программами безопасности на карантин или в резервное хранилище, а также с файлами, обработка которых отложена программами безопасности.

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

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

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в программе на территории США.

Аппаратные и программные требования

Сервер администрирования

Минимальные аппаратные требования:

- Процессор с частотой 1,4 ГГц или выше.
- Оперативная память: 4 ГБ.
- Объем свободного места на диске: требуется 10 ГБ для папки, где хранятся данные Сервера администрирования (/var/opt/kaspersky/klnagent_srv).

Поддерживаются следующие операционные системы:

- Debian GNU/Linux 11.x (Bullseye) 64-разрядная.
- Debian GNU/Linux 10.x (Buster) 64-разрядная.
- Debian GNU/Linux 9.x (Stretch) 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.
- 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.10015-01 (очередное обновление 1.7) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Альт Сервер 10 64-разрядная.
- Альт Сервер 9.2 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

Рекомендуется использовать файловую систему EXT4 с параметрами по умолчанию.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware Workstation 16 Pro.
- Microsoft Hyper-V Server 2012 64-разрядная.
- Microsoft Hyper-V Server 2012 R2 64-разрядная.
- Microsoft Hyper-V Server 2016 64-разрядная.
- Microsoft Hyper-V Server 2019 64-разрядная.
- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 17.
- Kernel-based Virtual Machine (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 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
- MariaDB 10.4.x 32-разрядная/64-разрядная.
- MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
- MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.

Kaspersky Security Center 14 Web Console

Сервер Kaspersky Security Center 14 Web Console

Минимальные аппаратные требования:

- Процессор: 4 ядра, частота от 2,5 ГГц.
- Оперативная память: 8 ГБ.
- Объем свободного места на диске: 40 ГБ (/var/opt/kaspersky).

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

- Debian GNU/Linux 11.x (Bullseye).
- Debian GNU/Linux 10.x (Buster).
- Debian GNU/Linux 9.x (Stretch).
- Ubuntu Server 20.04 LTS (Focal Fossa).
- Ubuntu Server 18.04 LTS (Bionic Beaver).
- CentOS 7.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).
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-разрядная.
- EulerOS 2.0 SP8 ARM.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
- Astra Linux Common Edition (очередное обновление 2.12).
- Альт Сервер 10.
- Альт Сервер 9.2.
- Альт 8 СП Сервер (ЛКНВ.11100-01).
- Альт 8 СП Сервер (ЛКНВ.11100-02).
- Альт 8 СП Сервер (ЛКНВ.11100-03).
- Oracle Linux 8.
- Oracle Linux 7.
- РЕД ОС 7.3 Сервер.
- РЕД ОС 7.3 Сертифицированная редакция.
- Kernel-based Virtual Machine (все операционные системы Linux, поддерживаемые Сервером Kaspersky Security Center 14 Web Console).

Клиентские устройства

Клиентскому устройству для работы с Kaspersky Security Center 14 Web Console требуется только браузер.

Минимальное разрешение экрана составляет 1366x768 пикселей.

Требования к аппаратному и программному обеспечению устройства соответствуют требованиям браузера, который используется для работы с Kaspersky Security Center 14 Web Console.

Браузеры:

- Mozilla Firefox Extended Support Release 91.8.0 или более поздняя версия (релиз 91.8.0 выпущен 5 апреля 2022).
- Mozilla Firefox Release 99.0 или более поздняя версия (релиз 99.0 выпущен 5 апреля 2022).
- Google Chrome 100.0.4896.88 или более поздняя версия (официальная сборка).
- Microsoft Edge 100 или более поздняя версия.
- Safari 15 для macOS.

Агент администрирования

Минимальные аппаратные требования:

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

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

Поддерживаются следующие операционные системы:

- Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная.
- Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная.
- Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная.
- Ubuntu Server 20.04 LTS (Focal Fossa) 32-разрядная/64-разрядная.
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64-разрядная.
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32-разрядная/64-разрядная.
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-разрядная/64-разрядная.
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-разрядная/64-разрядная.
- CentOS 8.x 64-разрядная.
- CentOS 7.x 64-разрядная.
- CentOS 7.x ARM 64-разрядная.
- Red Hat Enterprise Linux Server 8.x 64-разрядная.
- Red Hat Enterprise Linux Server 7.x 64-разрядная.
- Red Hat Enterprise Linux Server 6.x 32-разрядная/64-разрядная.
- SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Desktop 15 (все пакеты обновлений) 64-разрядная.
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64-разрядная.
- openSUSE 15 64-разрядная.
- EulerOS 2.0 SP8 ARM.
- Pardus OS 19.1 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7) ARM 64-разрядная.
- Альт Сервер 10 64-разрядная.
- Альт Сервер 9.2 64-разрядная.
- Альт Рабочая станция 10 32-разрядная/64-разрядная.
- Альт Рабочая станция 9.2 32-разрядная/64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
- Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-01) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-02) 32-разрядная/64-разрядная.
- Альт 8 СП Рабочая станция (ЛКНВ.11100-03) 32-разрядная/64-разрядная.
- Mageia 4 32-разрядная.

- Oracle Linux 7 64-разрядная.
- Oracle Linux 8 64-разрядная.
- Linux Mint 19.x 32-разрядная.
- Linux Mint 20.x 64-разрядная.
- AlterOS 7.5 или более поздняя версия 64-разрядная.
- ГосЛинукс IC6 64-разрядная.
- РЕД ОС 7.3 Сервер 64-разрядная.
- РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- ROSA Enterprise Linux Server 7.3 64-разрядная.
- ROSA Linux Enterprise Desktop 7.3 64-разрядная.
- РОСА "КОБАЛЬТ" Рабочая станция 7.3 64-разрядная.
- РОСА "КОБАЛЬТ" Сервер 7.3 64-разрядная.
- Лотос (версия ядра Linux 4.19.50, DE: MATE) 64-разрядная.

Поддерживаются следующие платформы виртуализации:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware Workstation 16 Pro.
- Microsoft Hyper-V Server 2012 64-разрядная.
- Microsoft Hyper-V Server 2012 R2 64-разрядная.
- Microsoft Hyper-V Server 2016 64-разрядная.
- Microsoft Hyper-V Server 2019 64-разрядная.
- Microsoft Hyper-V Server 2022 64-разрядная.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Kernel-based Virtual Machine (все операционные системы Linux, поддерживаемые Агентом администрирования).

Рекомендуется устанавливать ту же версию Агента администрирования для Linux, что и Kaspersky Security Center Linux.

О Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console представляет собой программу (веб-приложение), предназначенную для контроля состояния системы безопасности сетей организации, находящихся под защитой программ "Лаборатории Касперского".

С помощью программы вы можете выполнять следующие действия:

- контролировать состояние системы безопасности вашей организации;
- устанавливать программы "Лаборатории Касперского" на устройства вашей сети и управлять установленными программами;
- управлять политиками, сформированными для устройств вашей сети;
- управлять учетными записями пользователей;
- управлять задачами программ, установленных на устройствах сети;
- просматривать отчеты о состоянии системы безопасности;

- управлять рассылкой отчетов заинтересованным лицам: системным администраторам и другим IT-специалистам.

Kaspersky Security Center 14 Web Console предоставляет веб-интерфейс, который обеспечивает ваше взаимодействие с Сервером администрирования с помощью браузера. Сервер администрирования – это программа, которая служит для управления программами "Лаборатории Касперского", установленными на устройства вашей сети. Сервер администрирования связывается с устройствами вашей сети через защищенные (SSL) каналы связи. Когда вы с помощью браузера подключаетесь к Kaspersky Security Center 14 Web Console, браузер устанавливает с Сервером Kaspersky Security Center 14 Web Console защищенное (HTTPS) соединение.

Kaspersky Security Center 14 Web Console работает следующим образом:

1. Вы подключаетесь к Kaspersky Security Center 14 Web Console с помощью браузера, в окне которого отображаются страницы веб-портала программы.

2. С помощью элементов управления веб-портала вы выбираете команду, которую хотите выполнить. Kaspersky Security Center 14 Web Console выполняет следующие действия:

   - Если вы выбрали команду, связанную с получением информации (например, просмотр списка устройств), Kaspersky Security Center 14 Web Console формирует запрос на получение информации к Серверу администрирования, затем получает от него необходимые данные и передает их браузеру в удобном для отображения виде.

   - Если вы выбрали команду управления (например, удаленная установка программы), Kaspersky Security Center 14 Web Console получает команду от браузера и передает ее Серверу администрирования. Затем программа получает результат выполнения команды от Сервера администрирования и передает результат браузеру в удобном для отображения виде.

Kaspersky Security Center 14 Web Console представляет собой многоязыковую программу. Вы можете изменить язык интерфейса в любое время без повторного открытия программы. Если вы устанавливаете Kaspersky Security Center 14 Web Console совместно с Kaspersky Security Center, Kaspersky Security Center 14 Web Console имеет тот же язык интерфейса что и установочный файл. Если вы устанавливаете только Kaspersky Security Center 14 Web Console, программа имеет тот же язык что и операционная система. Если Kaspersky Security Center 14 Web Console не поддерживает язык установочного файла или операционной системы, по умолчанию устанавливается английский язык.

Совместимые программы и решения "Лаборатории Касперского"

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

- Kaspersky Endpoint Security для Linux

- Kaspersky Industrial CyberSecurity for Linux Nodes

Эти программы позволяют защитить как рабочие станции, так и файловые серверы. Подробнее о версиях программ и решений см. на странице "Жизненный цикл программ".

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

"Лаборатория Касперского" предлагает программу Kaspersky Security Center в качестве локального решения для двух платформ – Windows и Linux. В решении для Windows вы устанавливаете Сервер администрирования на устройство с операционной системой Windows. Решение на базе Linux имеет версию Сервера администрирования, предназначенную для установки на устройство с операционной системой Linux. Эта онлайн-справка содержит информацию о Kaspersky Security Center Linux. Для получения подробной информации о решении на базе Windows см. справку Kaspersky Security Center Windows.

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

Сравнение возможностей программы Kaspersky Security Center на базе Windows и на базе Linux

Функция или свойство	Kaspersky Security Center 14	
	Решение на базе Windows	Решение на базе Linux
Расположение Сервера администрирования	В локальной инфраструктуре	В локальной инфраструктуре
Расположение системы управления базами данных (СУБД)	В локальной инфраструктуре	В локальной инфраструктуре
Операционная система для установки Сервера администрирования	Windows	Linux
Тип Консоли администрирования	Локальная и веб-интерфейс	Веб-интерфейс
Операционная система для установки Консоли администрирования с веб-интерфейсом	Windows или Linux	Windows или Linux
Иерархия Серверов администрирования	✓	✓
Иерархия групп администрирования	✓	✓

Опрос сети	✓	✓ (только по IP-диапазонам)
Максимальное количество управляемых устройств	100 000	20 000
Защита устройств под управлением Windows, macOS и Linux	✓	— (только защита устройств с операционной системой Linux)
Защита мобильных устройств	✓	—
Защита виртуальных машин	✓	—
Защита публичной облачной инфраструктуры	✓	—
Управление безопасностью устройств	✓	✓
Управление безопасностью, ориентированной на пользователя	✓	✓
Политики программ	✓	✓
Задачи для программ "Лаборатории Касперского"	✓	✓
Kaspersky Security Network	✓	—
Прокси-сервер KSN	✓	—
Kaspersky Private Security Network	✓	—
Централизованное распространение лицензионных ключей программ "Лаборатории Касперского"	✓	✓
Поддержка виртуальных Серверов администрирования	✓	✓
Установка обновлений программ сторонних производителей и поиск уязвимостей в программах сторонних производителей	✓	— (только с помощью задачи удаленной установки)
Уведомления о событиях, произошедших на управляемых устройствах	✓	✓
Создание учетных записей пользователей, контроль учетных записей	✓	✓
Мониторинг состояния политик и задач	✓	✓
Развертывание отказоустойчивого кластера Kaspersky Security Center	✓	✓

Основные понятия

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

Сервер администрирования

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

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

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

- 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.

Сервер администрирования выполняет следующие функции:

- хранение структуры групп администрирования;
- хранение информации о конфигурации клиентских устройств;
- организация хранилищ дистрибутивов программ;
- удаленная установка программ на клиентские устройства и удаление программ;

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

Правило именования Серверов администрирования в интерфейсе программы

В интерфейсе Kaspersky Security Center 14 Web Console Серверы администрирования могут иметь следующие имена:

- Имя устройства Сервера администрирования, например: "*имя_устройства*" или "Сервер администрирования: *имя_устройства*".
- IP-адрес устройства Сервера администрирования, например: "*IP_адрес*" или "Сервер администрирования: *IP_адрес*".
- Подчиненные Серверы администрирования и виртуальные Серверы администрирования имеют собственные имена, которые вы указываете при подключении виртуального или подчиненного Сервера администрирования к главному Серверу администрирования.
- Если вы используете программу Kaspersky Security Center 14 Web Console, установленную на устройство под управлением Linux, то программа отображает имена Серверов администрирования, которые вы указали как доверенные в файле ответов.

Вы можете подключиться к Серверу администрирования с помощью Kaspersky Security Center 14 Web Console.

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.

Частным случаем подчиненных Серверов администрирования являются *виртуальные Серверы администрирования*.

В иерархии Сервер администрирования Kaspersky Security Center Linux может работать только как подчиненный Сервер под управлением главного Сервера администрирования Kaspersky Security Center на базе Windows или Kaspersky Security Center Cloud Console.

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 14 Web Console. Для управления большим числом клиентских устройств различных организаций поставщик услуг может включать в иерархию Серверов администрирования виртуальные Серверы администрирования.

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.

Виртуальный Сервер администрирования

Виртуальный Сервер администрирования (далее также *виртуальный Сервер*) – компонент программы 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 программ "Лаборатории Касперского" на клиентские устройства, работающие под управлением виртуального Сервера, необходимо, чтобы на одном из клиентских устройств был установлен Агент администрирования для связи с виртуальным Сервером. При первом подключении к виртуальному Серверу администрирования это устройство автоматически назначается точкой распространения и выполняет роль шлюза соединений клиентских устройств с виртуальным Сервером администрирования.
- Виртуальный Сервер администрирования может опрашивать сеть только через точки распространения.
- Чтобы перезапустить виртуальный Сервер, работоспособность которого была нарушена, Kaspersky Security Center Linux 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. 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.

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

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 устройство этого сотрудника из группы администрирования "Бухгалтеры" в группу администрирования "Разработчики". Таким образом, устройству будут автоматически переданы параметры программы, 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 программ, установленных на устройствах. Вы также можете формировать отчеты для управляемых устройств.

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

Устройство может находиться под управлением только одного Сервера администрирования. Один Сервер администрирования может обслуживать до 20 000 устройств.

Нераспределенное устройство

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

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

Рабочее место администратора

Устройства, на которых установлен Сервер Kaspersky Security Center 14 Web Console, называются *рабочими местами администраторов*. С этих устройств администраторы могут осуществлять удаленное централизованное управление программами "Лаборатории Касперского", установленными на клиентских устройствах.

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

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

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

Веб-плагин управления

Веб-плагин управления – это специальный компонент, используемый для удаленного управления программами "Лаборатории Касперского" с помощью Kaspersky Security Center 14 Web Console. Веб-плагин управления также называется *плагином управления*. Плагин управления представляет собой интерфейс между Kaspersky Security Center 14 Web Console и определенной программой "Лаборатории Касперского". С помощью плагина управления можно настраивать задачи и политики для программы.

Вы можете загрузить веб-плагины управления с веб-сайта Службы технической поддержки "Лаборатории Касперского".

Плагин управления предоставляет следующие возможности:

- Интерфейс для создания и изменения задач и параметров программы.
- Интерфейс для создания и изменения политик и профилей политик для удаленной централизованной настройки программ "Лаборатории Касперского" и устройств.
- Передачу событий, сформированных программами.
- Функции Kaspersky Security Center 14 Web Console для отображения оперативных данных и событий программы, а также статистики, полученной от клиентских устройств.

Политики

Политика – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько программ "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждой программы "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

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

Политики действуют по следующим правилам:

- Для одной программы можно настроить несколько политик с различными значениями.
- Для одной программы может быть активна только одна политика.
- Политика может иметь дочерние политики.

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

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

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

Профили политик работают по следующим правилам:

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

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.

Задачи

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

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

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

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 14 Web Console, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

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

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

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

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

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

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

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

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

Область действия задачи

Область задачи – 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 программы

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

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

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

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

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

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

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

Точка распространения

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

> Функции и варианты использования Агента администрирования, установленного на устройстве, которое выполняет роль точки распространения, изменяются в зависимости от операционной системы.

Точка распространения может выполнять следующие функции:

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

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

- Распространять политики и групповые задачи с помощью широковещательной рассылки по протоколу UDP.
- Выполнять роль шлюза соединений с Сервером администрирования для устройств группы администрирования.

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

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

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

- Осуществлять удаленную установку программ "Лаборатории Касперского" и других поставщиков программного обеспечения, в том числе установку на клиентские устройства без Агента администрирования.

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

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

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

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

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

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

Агенты администрирования с активным профилем соединения не участвуют в определении широковещательного домена.

Kaspersky Security Center Linux присваивает каждому Агенту администрирования уникальный адрес многоадресной IP-рассылки, который не пересекается с другими адресами. Это позволяет избежать превышения нагрузки на сеть, которое возникло бы из-за пересечения адресов. Адреса многоадресной IP-рассылки, уже присвоенные в прошлых версиях программы, изменены не будут.

Если на одном участке сети или в группе администрирования назначаются две точки распространения или более, одна из них становится активной точкой распространения, остальные назначаются резервными. Активная точка распространения загружает обновления и инсталляционные пакеты непосредственно с Сервера администрирования, резервные точки распространения обращаются за обновлениями только к активной точке распространения. В этом случае файлы загружаются только один раз с Сервера администрирования и далее распределяются между точками распространения. Если активная точка распространения по каким-либо причинам становится недоступной, одна из резервных точек распространения назначается активной. Сервер администрирования назначает точку распространения резервной автоматически.

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

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

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

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

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

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.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security Center 14 Linux.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского" в котором указано, на каких условиях вы можете использовать программу.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Kaspersky Security Center Linux и его компоненты, например Агент администрирования, имеют собственные Лицензионные соглашения.

Вы можете ознакомиться с условиями Лицензионного соглашения для Kaspersky Security Center Linux 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".

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.

  Обратите внимание, что при установке Агента администрирования для Linux, Лицензионное соглашение для Агента администрирования отображается на английском языке. Вы можете ознакомиться с Лицензионным соглашением для Агента администрирования на других языках в папке /opt/kaspersky/klnagent64/share/license перед тем, как принять условия Лицензионного соглашения во время установки.

- 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".

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки программы. Если вы не согласны с условиями Лицензионного соглашения, вы должны прервать установку программы и не должны использовать программу.

О лицензии

Лицензия – это ограниченное по времени право на использование Kaspersky Security Center Linux, предоставляемое вам на основании Лицензионного соглашения.

Объем предоставляемых услуг и срок использования программы зависят от лицензии, по которой используется программа.

Предусмотрены следующие типы лицензий:

- *Пробная.*

  Бесплатная лицензия, предназначенная для ознакомления с программой. Пробная лицензия имеет небольшой срок действия.

  По истечении срока действия пробной лицензии Kaspersky Security Center Linux прекращает выполнять все свои функции. Чтобы продолжить использование программы, вам нужно приобрести коммерческую лицензию.

  Вы можете использовать программу по пробной лицензии только в течение одного пробного периода.

- *Коммерческая.*

  Платная лицензия.

  По истечении срока действия коммерческой лицензии программа прекращает выполнять свои основные функции. Чтобы продолжить использование Kaspersky Security Center, вам нужно продлить срок действия коммерческой лицензии. По истечении срока действия коммерческой лицензии вы не сможете продолжать использовать программу и должны удалить ее со своего устройства.

  Рекомендуется продлевать срок действия лицензии не позднее даты его окончания, чтобы обеспечить непрерывную защиту от угроз компьютерной безопасности.

О лицензионном сертификате

Лицензионный сертификат – это документ, который передается вам вместе с файлом ключа или кодом активации.

В Лицензионном сертификате содержится следующая информация о предоставляемой лицензии:

- лицензионный ключ или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о программе, которую можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, устройств, на которых можно использовать программу по предоставляемой лицензии);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

О лицензионном ключе

Лицензионный ключ – последовательность бит, с помощью которой вы можете активировать и затем использовать программу в соответствии с условиями Лицензионного соглашения. Лицензионный ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить лицензионный ключ в программу одним из следующих способов: применить *файл ключа* или ввести *код активации*. Лицензионный ключ отображается в интерфейсе программы в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

Лицензионный ключ может быть заблокирован "Лабораторией Касперского", если условия Лицензионного соглашения нарушены. Если лицензионный ключ заблокирован, для работы программы требуется добавить другой лицензионный ключ.

Лицензионный ключ может быть активным и дополнительным (резервным).

Активный лицензионный ключ – лицензионный ключ, используемый в текущий момент для работы программы. В качестве активного может быть добавлен лицензионный ключ для пробной или коммерческой лицензии. В программе не может быть больше одного активного лицензионного ключа.

Дополнительный (резервный) лицензионный ключ – лицензионный ключ, подтверждающий право на использование программы, но не используемый в текущий момент. Дополнительный лицензионный ключ автоматически становится активным, когда заканчивается срок действия лицензии, связанной с текущим активным лицензионным ключом. Дополнительный лицензионный ключ может быть добавлен только при наличии активного лицензионного ключа.

Лицензионный ключ для пробной лицензии может быть добавлен только в качестве активного лицензионного ключа. Лицензионный ключ для пробной лицензии не может быть добавлен в качестве дополнительного лицензионного ключа.

Просмотр Политики конфиденциальности

Политика конфиденциальности доступна в интернете на странице https://www.kaspersky.ru/products-and-services-privacy-policy.

Политика конфиденциальности также доступна в автономном режиме:

- Вы можете ознакомиться с Политикой конфиденциальности перед установкой Kaspersky Security Center.
- Текст Политики конфиденциальности находится в файле license.txt в папке установки Kaspersky Security Center.
- Файл privacy_policy.txt доступен на управляемом устройстве в папке Агента администрирования.
- Вы можете распаковать файл privacy_policy.txt из дистрибутива Агента администрирования.

Варианты лицензирования Kaspersky Security Center

Kaspersky Security Center поставляется в составе программ "Лаборатории Касперского" для защиты корпоративных сетей. Кроме того, она доступна для загрузки с веб-сайта "Лаборатории Касперского".

Доступны следующие функции:

- создание виртуальных Серверов администрирования для управления сетью удаленных офисов или организаций-клиентов;
- формирование иерархии групп администрирования для управления набором устройств как единым целым;
- контроль состояния антивирусной безопасности организации;
- удаленная установка программ;
- просмотр списка образов операционных систем, доступных для удаленной установки;
- централизованная настройка параметров программ, установленных на клиентских устройствах;
- получение статистики и отчетов о работе программ, а также уведомлений о критических событиях;
- просмотр и редактирование вручную списка оборудования, обнаруженного в результате опроса сети;
- централизованная работа с файлами, помещенными на карантин или в резервное хранилище, а также с файлами, обработка которых отложена;
- управление ролями пользователей.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления лицензионного ключа, активирующего программу.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения Kaspersky Security Center или после заказа пробной версии Kaspersky Security Center.

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

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- обратиться к продавцу лицензии;
- получить файл ключа на веб-сайте "Лаборатории Касперского" на основе имеющегося кода активации;

О предоставлении данных

Передача данных Правообладателю

Перечислены в Лицензионном соглашении Kaspersky Security Center 14 Linux.

Данные, обрабатываемые локально

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

- обнаружение устройств и их пользователей в сети организации;
- формирование иерархии групп администрирования для управления устройствами;
- установка программ "Лаборатории Касперского" на устройства;
- управление параметрами работы и задачами установленных программ;
- активация программ "Лаборатории Касперского" на устройствах;
- управление учетными записями пользователей;
- просмотр информации о работе программ "Лаборатории Касперского" на устройствах;
- просмотр отчетов.

Для выполнения своих основных функций программа Kaspersky Security Center Linux может принимать, хранить и обрабатывать следующую информацию:

- Данные об устройствах в сети организации, полученные в результате обнаружения устройств в сети или проверки IP-диапазонов. Сервер администрирования самостоятельно получает данные или их передает ему Агент администрирования.
- 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 14 Web Console:
  - Технические характеристики управляемого устройства и его компонентов, необходимые для идентификации устройства: отображаемое имя и описание устройства, DNS-домен и DNS-имя, IPv4-адрес, IPv6-адрес, сетевое местоположение, MAC-адрес, тип операционной системы, является ли устройство виртуальной машиной и тип гипервизора, является ли устройство динамической виртуальной машиной как частью VDI.
  - Прочие характеристики управляемых устройств и их компонентов, необходимые для аудита управляемых устройств: архитектура операционной системы, поставщик операционной системы, номер сборки операционной системы, идентификатор выпуска операционной системы, папка расположения операционной системы, если устройство является виртуальной машиной, то тип виртуальной машины.
  - Подробные данные о действиях на управляемых устройствах: дата и время последнего обновления, время, когда устройство последний раз было видимо в сети, состояние ожидания перезапуска, время включения устройства.
  - Данные об учетных записях пользователей устройств и их сеансах работы.
- Статистику работы точки распространения, если устройство является точкой распространения. Агент администрирования передает данные от устройства на Сервер администрирования.
- Параметры точки распространения, которые Пользователь вводит в Kaspersky Security Center 14 Web Console.
- Данные о программах "Лаборатории Касперского", установленных на устройстве. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования:
  - Параметры программ "Лаборатории Касперского", установленных на управляемом устройстве: название и версия программы "Лаборатории Касперского", статус, состояние постоянной защиты, дата и время последней проверки устройства, количество обнаруженных угроз, количество объектов, для которых не удалось выполнить лечение, наличие и статус компонентов программы, данные о параметрах и задачах программы "Лаборатории Касперского", информация об активном и резервных лицензионных ключах, дата и идентификатор установки программы.
  - Статистика работы программы: события, связанные с изменениями статуса компонентов программы "Лаборатории Касперского" на управляемом устройстве и с выполнением задач, инициированных программными компонентами.
  - Состояние устройства, определенное программой "Лаборатории Касперского".
  - Теги, передаваемые программой "Лаборатории Касперского".
- Данные, содержащиеся в событиях от компонентов Kaspersky Security Center Linux и управляемых программ "Лаборатории Касперского". Агент администрирования передает данные от устройства на Сервер администрирования.
- Настройки компонентов Kaspersky Security Center Linux и управляемых программ "Лаборатории Касперского", представленные в виде политик и профилей политик. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.

- Настройки задач компонентов Kaspersky Security Center Linux и управляемых программ "Лаборатории Касперского". Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Данные, обрабатываемые функцией Системное администрирование. Агент администрирования передает с устройства на Сервер администрирования информацию об оборудовании, обнаруженном на управляемых устройствах (Реестр оборудования).
- Пользовательские категории программ. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Данные об исполняемых файлах, обнаруженных на управляемых устройствах функцией Контроль программ. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о файлах, помещенных в резервное хранилище. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о файлах, помещенных в Карантин. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о файлах, запрошенных специалистами "Лаборатории Касперского" для подробного анализа. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о внешних устройствах (устройствах памяти, инструментах передачи информации, инструментах превращения информации в твердую копию, шинах подключения), установленных или подключенных к управляемому устройству и обнаруженных функцией Контроль устройств. Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Список управляемых программируемых логических контроллеров (ПЛК). Управляемая программа передает данные с устройства на Сервер администрирования через Агент администрирования. Полный список данных представлен в справке соответствующей программы.
- Данные о введенных активационных кодах. Пользователь вводит данные в интерфейсе Консоли администрирования или Kaspersky Security Center 14 Web Console.
- Учетные записи пользователей: имя, описание, полное имя, адрес электронной почты, основной телефон, пароль. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Истории ревизий объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Реестр удаленных объектов управления. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Инсталляционные пакеты, созданные из файла, и параметры установки. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Данные, необходимые для отображения объявлений от "Лаборатории Касперского" в Kaspersky Security Center 14 Web Console. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Данные, необходимые для работы плагинов управляемых программ в Kaspersky Security Center 14 Web Console и сохраняемые плагинами в базе данных Сервера администрирования в процессе повседневной работы. Описание и способы предоставления данных приведены в файлах справки соответствующей программы.
- Настройки пользователя Kaspersky Security Center 14 Web Console: язык локализации и тема пользовательского интерфейса, настройки отображения панели мониторинга, информации о состоянии нотификаций (прочитано/не прочитано), состояние столбцов в таблицах (скрыть/показать), прогресс прохождения режима обучения. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Сертификат безопасного подключения управляемых устройств к компонентам Kaspersky Security Center Linux. Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Любые данные, которые Пользователь вводит в интерфейсе Kaspersky Security Center 14 Web Console.
- Любые данные, которые Пользователь вводит в интерфейсе Kaspersky Security Center 14 Web Console.

Перечисленные выше данные могут попасть в Kaspersky Security Center Linux следующими способами:

- Пользователь вводит данные в интерфейсе Kaspersky Security Center 14 Web Console.
- Агент администрирования самостоятельно получает данные с устройства и передает на Сервер администрирования.
- Агент администрирования получает собранные управляемой программой "Лаборатории Касперского" данные и передает на Сервер администрирования. Перечни данных, обрабатываемых управляемыми программами "Лаборатории Касперского", приведены в справках соответствующих программ.
- Сервер администрирования самостоятельно получает 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 Linux, включая файлы журналов, создаваемые инсталляторами и утилитами.

"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 14 Web Console, Пользователь соглашается на автоматическую передачу следующих данных:

- код Kaspersky Security Center Linux;
- версия Kaspersky Security Center Linux;
- локализация Kaspersky Security Center Linux;
- 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 Linux – это заказ на использование программы с выбранными параметрами (дата окончания подписки, количество защищаемых устройств). Подписку на Kaspersky Security Center Linux можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security Center после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность программы сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security Center Linux по подписке, требуется применить код активации, предоставленный поставщиком услуг.

Вы можете применить другой код активации для использования Kaspersky Security Center Linux только после окончания подписки или отказа от нее.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность программы сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security Center.

При использовании программы по подписке Kaspersky Security Center Linux автоматически обращается к серверу активации через определенные промежутки времени вплоть до даты окончания подписки. Если доступ к серверу через системный DNS невозможен, программа использует публичные DNS-серверы. Вы можете продлить подписку на веб-сайте поставщика услуг.

События превышения лицензионного ограничения

Kaspersky Security Center Linux позволяет получать информацию о событиях превышения лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах.

Уровень важности событий о превышении лицензионного ограничения определяется по следующим правилам:

- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 90%–100% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Информационное сообщение**.
- Если количество используемых лицензионных единиц одной лицензии лежит в интервале 100%–110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Предупреждение**.
- Если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц этой лицензии, публикуется событие с уровнем важности **Критическое событие**.

Архитектура программы

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

Архитектура программы Kaspersky Security Center 14 Linux

Программа Kaspersky Security Center 14 Linux включает в себя следующие основные компоненты:

- **Kaspersky Security Center 14 Web Console**. Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.
- **Сервер администрирования Kaspersky Security Center** (далее также *Сервер*). Осуществляет функции централизованного хранения информации об установленных в сети организации программах и управления ими.
- **Серверы обновлений "Лаборатории Касперского"**. HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.
- **Клиентские устройства.** Клиентские устройства организации защищены Kaspersky Security Center 14 Linux. На каждом защищаемом устройстве должна быть установлена одна из программ безопасности "Лаборатории Касперского".

Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console

На следующем рисунке приведена схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console.

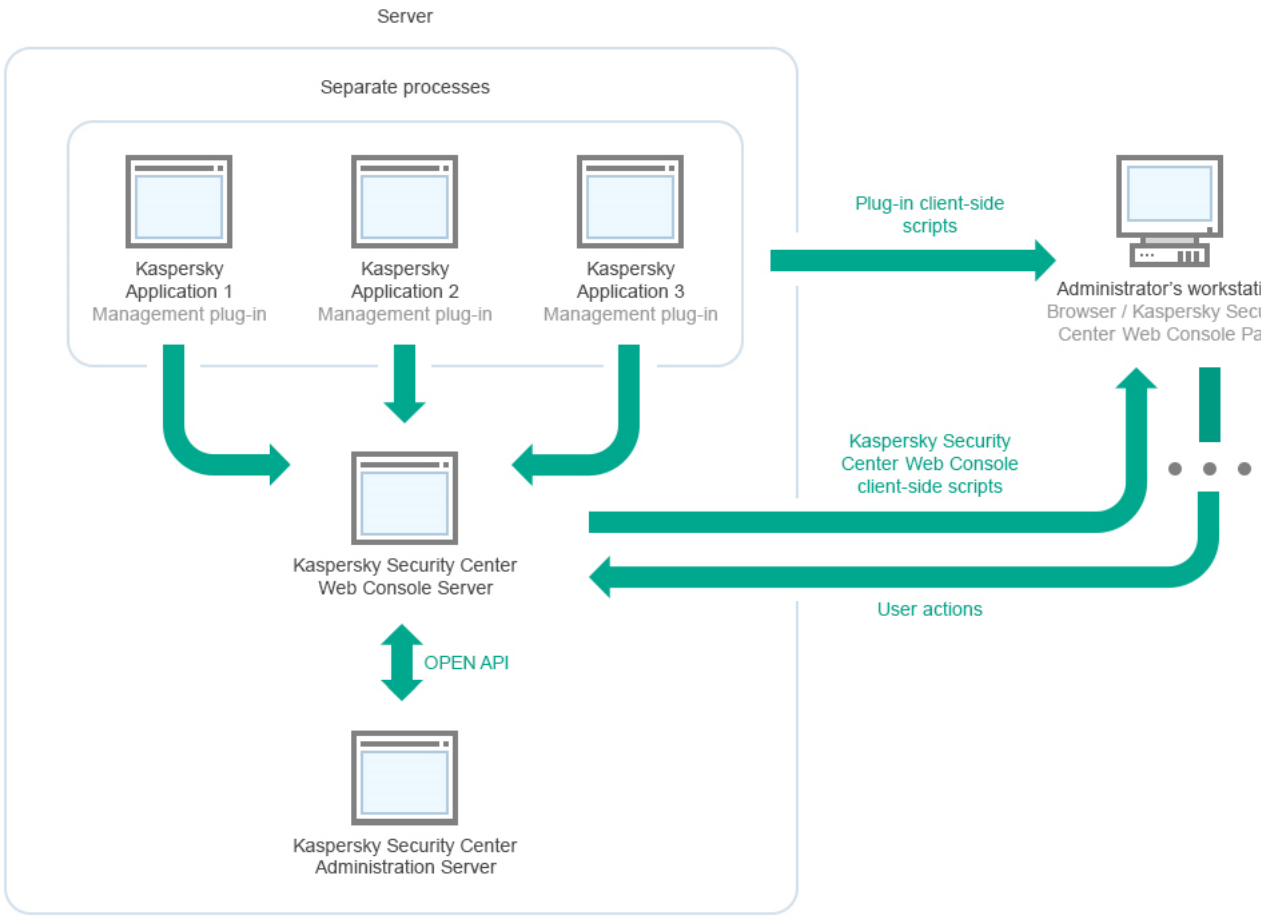


Схема развертывания Сервера администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console

Развертывание плагинов управления программами "Лаборатории Касперского", установленных на защищаемых устройствах (отдельный плагин для каждой программы), происходит одновременно с развертыванием Сервера Kaspersky Security Center 14 Web Console.

Как администратор, вы имеете доступ к Kaspersky Security Center 14 Web Console через браузер на вашей рабочей станции.

Когда вы выполняете определенные действия в Kaspersky Security Center 14 Web Console, Сервер Kaspersky Security Center 14 Web Console взаимодействует с Сервером администрирования Kaspersky Security Center по OpenAPI. Сервер Kaspersky Security Center 14 Web Console запрашивает необходимые данные у Сервера администрирования Kaspersky Security Center и отображает результаты ваших действий в Kaspersky Security Center 14 Web Console.

Порты, используемые Kaspersky Security Center Linux

В таблицах ниже показаны порты по умолчанию, используемые Сервером администрирования и клиентскими устройствами. При необходимости вы можете изменить каждый из этих портов по умолчанию.

Порты, используемые Сервером администрирования Kaspersky Security Center Linux

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. Этот порт является необязательным. В целях безопасности рекомендуется использовать TCP-порт 8061.
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;	Управление клиентскими устройствами и подчиненными Серверами администрирования.

			используется также на подчиненных серверах для приема подключений от главного Сервера (например, если подчиненный Сервер находится в демилитаризованной зоне)	Вы можете изменить номер порта по умолчанию для приема подключений от Агентов администрирования при настройке портов подключения во время установки Kaspersky Security Center Linux. Вы можете изменить номер порта по умолчанию для приема подключений от подчиненных Серверов администрирования при создании иерархии Серверов администрирования.
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.
13291	klserver	TCP (TLS)	Прием подключений от Консоли администрирования к Серверу администрирования	Управление Сервером администрирования. По умолчанию порт закрыт. Если вы хотите использовать утилиту klakaut для автоматизации работы Kaspersky Security Center Linux, откройте порт 13291 с помощью утилиты klscflag.
13299	klserver	TCP (TLS)	Получение соединений от Kaspersky Security Center 14 Web Console к Серверу администрирования; получение соединений от Сервера администрирования через OpenAPI	Kaspersky Security Center 14 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.
14000	klserver	TCP	Прием подключений от Агентов администрирования	Управление клиентскими устройствами. Вы можете изменить номер порта по умолчанию при настройке портов подключения при установке Kaspersky Security Center Linux или при подключении клиентского устройства к Серверу администрирования вручную. Этот порт является необязательным. В целях безопасности рекомендуется использовать TCP-порт 1300.
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.
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.
17000	klactprx	TCP (TLS)	Прием подключений для активации программ от управляемых устройств	Прокси-сервер активации для управляемых устройств. Вы можете изменить номер порта по умолчанию в окне свойств Сервера администрирования (в подразделе **Дополнительные порты** раздела **Общий**).

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

В таблице ниже указан порт, который используется Сервером Kaspersky Security Center 14 Web Console. Это может быть то же устройство, на котором установлен Сервер администрирования, или другое устройство.

Порт, используемый Сервером Kaspersky Security Center 14 Web Console

Номер порта	Имя процесса, открывающего порт	Протокол	Назначение порта	Область
8080	Node.js: серверный JavaScript	TCP (TLS)	Прием соединений от браузера и передача в Kaspersky Security Center 14 Web Console	Kaspersky Security Center 14 Web Console. Вы можете изменить номер порта, указанного по умолчанию, во время установки Kaspersky Security Center 14 Web Console. Если вы устанавливаете Kaspersky Security Center 14 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 используется управляемыми устройствами с установленным Агентом администрирования.

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.
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.
30522, 30523 (порты в интерфейсе localhost)	klnagent	TCP	Получение обновлений программ "Лаборатории Касперского" с Сервера администрирования с помощью компонента FileTransferBridge	Управляемые устройства, которые получают обновления программы "Лаборатории Касперского" с Сервера администрирования, указанного в качестве источника обновлений баз.

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 Linux 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 используются управляемыми устройствами с установленным Агентом администрирования, выполняющими роль точек распространения. Перечисленные порты используются устройствами, выполняющими роль точек распространения, в дополнение к портам, используемым Агентами администрирования (см. таблицу выше).

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	Управление клиентскими устройствами, доставка обновлений и инсталляционных пакетов. Вы можете изменить значения портов по умолчанию в свойствах точки распространения.
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.
15111 (только если на устройстве запущена служба прокси-	ksnproxy	UDP	Прием запросов от управляемых устройств к	Прокси-сервер KSN.

сервера KSN)	прокси-серверу KSN	Вы можете изменить значения портов по умолчанию в свойствах точки распространения.

Порты, используемые программой Kaspersky Security Center 14 Web Console

В таблице ниже перечислены порты, которые должны быть открыты на устройстве, на котором установлен Сервер Kaspersky Security Center 14 Web Console (далее также просто Kaspersky Security Center 14 Web Console).

Порты, используемые программой Kaspersky Security Center 14 Web Console

Номер порта	Имя службы	Протокол	Назначение порта	Область
2001	Kaspersky Security Center Product Plugins Server	HTTPS	API-порт, который используется процессами плагина управления для приема запросов от службы Kaspersky Security Center Web Console Management Service	Запуск процессов node плагинов управления.
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	API-порты, которые используются для получения запросов от службы Kaspersky Security Center Web Console Management Service, работающей на том же устройстве	Обновление компонентов Kaspersky Security Center 14 Web Console.
2005	Kaspersky Security Center Web Console	HTTPS	API-порт, который используется для получения запросов от службы Kaspersky Security Center Web Console Management Service, работающей на том же устройстве.	Запуск процессов node программы Kaspersky Security Center 14 Web Console.
8200	—	HTTP	API-порт, который используется для генерации сертификатов с помощью HashiCorp Vault (подробнее см. на сайте HashiCorp Vault)	Установка Kaspersky Security Center 14 Web Console и обновление компонентов Kaspersky Security Center 14 Web Console.
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	API-порты Message Broker, которые используются для связи между Kaspersky Security Center 14 Web Console и плагинами управления.	Взаимодействие между Kaspersky Security Center 14 Web Console и плагинов управления

Установка

В этом разделе описана установка Kaspersky Security Center и Kaspersky Security Center 14 Web Console.

Основной сценарий установки

Следуя этому сценарию, вы установите Сервер администрирования Kaspersky Security Center 14 Linux и Kaspersky Security Center 14 Web Console, выполните первоначальную настройку Сервера администрирования с помощью мастера первоначальной настройки, а также установите программы "Лаборатории Касперского" на управляемые устройства с помощью мастера развертывания защиты.

Предварительные требования

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

Если вы хотите попробовать Kaspersky Security Center 14 Linux, вы можете получить пробную тридцатидневную версию на веб-сайте "Лаборатории Касперского" .

Этапы

Основной сценарий установки состоит из следующих этапов:

1. **Выбор структуры защиты организации**

   Ознакомьтесь с компонентами Kaspersky Security Center Linux. 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.

Определите, будет ли в вашей организации использоваться иерархия Серверов администрирования. 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 доверенным центром сертификации (CA), подготовьте эти сертификаты и убедитесь, что они соответствуют всем требованиям.

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

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

Вы можете выбрать одну из поддерживаемых СУБД.

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

Если вы используете MariaDB, необходимо настроить рекомендуемые параметры для оптимальной работы СУБД с Kaspersky Security Center.

4 **Настройка портов**

Убедитесь, что для взаимодействия компонентов согласно выбранной вами структуре защиты открыты необходимые порты.

Если требуется предоставить доступ к Серверу администрирования из интернета, 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, и установите на устройство Kaspersky Security Center. Вместе с компонентом Сервер администрирования автоматически будет установлена серверная версия Агента администрирования.

6 **Установка Kaspersky Security Center 14 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, и установите на это устройство Kaspersky Security Center 14 Web Console. Вы можете установить Kaspersky Security Center 14 Web Console на том же устройстве, что и Сервер администрирования.

Загрузите веб-плагин управления Kaspersky Endpoint Security для Linux и установите его на то же устройство, на котором установлена программа Kaspersky Security Center 14 Web Console.

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

По умолчанию программа не использует устройство с Сервером администрирования как управляемое устройство. Для защиты Сервера администрирования от вирусов и других угроз, а также для управления этим устройством рекомендуется установить Kaspersky Endpoint Security для Linux и Агент администрирования для Linux 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. Выполните первоначальную настройку Сервера администрирования в соответствии с вашими требованиями. На этапе первоначальной настройки мастер создает необходимые для развертывания защиты политики и задачи с параметрами по умолчанию. Эти параметры могут оказаться неоптимальными для нужд вашей организации. При необходимости вы можете изменить параметры политик и задач.

9 **Обнаружение сетевых устройств**

Опросите сеть для обнаружения устройств вручную. В результате Сервер администрирования Kaspersky Security Center Linux получает адреса и имена всех устройств, зарегистрированных в сети. В дальнейшем вы можете с помощью Kaspersky Security Center Linux устанавливать программы "Лаборатории Касперского" и других производителей на обнаруженные устройства. Kaspersky Security Center Linux 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 с учетом организационной структуры организации. Вы можете создать правила перемещения для распределения устройств по группам 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. Точки распространения рекомендуется использовать в больших сетях для снижения нагрузки на Сервер администрирования, а также в сетях с распределенной структурой для предоставления Серверу администрирования доступа к устройствам или группам устройств, соединенным каналами с низкой пропускной способностью.

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

    Развертывание защиты в сети организации подразумевает установку Агента администрирования и программ безопасности на устройства, найденные Сервером администрирования в процессе обнаружения устройств.

    Чтобы выполнить удаленную установку программы, запустите мастер развертывания защиты.

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

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

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

    Распространите лицензионные ключи на клиентские устройства, чтобы активировать управляемые программы безопасности на этих устройствах.

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

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

15. **Мониторинг состояния защиты сети**

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

Настройка сервера MariaDB x64 для работы с Kaspersky Security Center 14 Linux

Рекомендуемые параметры для файла my.cnf

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

Чтобы настроить файл my.cnf:

1. Откройте файл my.cnf 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. Убедитесь, что для параметра `innodb_file_per_table` установлено значение `1`.

   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 MySQL x64 для работы с Kaspersky Security Center 14 Linux

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

Рекомендуемые параметры для файла my.cnf

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

Чтобы настроить файл my.cnf:

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

2. Добавьте следующие строки в раздел `[mysqld]` файла my.cnf:

   ```
   sort_buffer_size=10M
   join_buffer_size=20M
   tmp_table_size=600M
   max_heap_table_size=600M
   key_buffer_size=200M
   innodb_buffer_pool_size= реальное значение должно быть не менее 80% от ожидаемого размера базы данных KAV
   innodb_thread_concurrency=20
   innodb_flush_log_at_trx_commit=0 (в большинстве случаев сервер использует небольшие транзакции)
   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
   ```

   Обратите внимание, что память, указанная в `innodb_buffer_pool_size`, выделяется при запуске сервера. Если размер базы данных меньше указанного размера буфера, выделяется только необходимая память. Фактический размер выделенной памяти примерно на 10 процентов превышает указанный размер буфера. Дополнительную информацию см. в документации MySQL.

   Рекомендуется использовать значение параметра `innodb_flush_log_at_trx_commit = 0`, поскольку значения "1" или "2" отрицательно влияют на скорость работы MySQL. Убедитесь, что для параметра `innodb_file_per_table` установлено значение `1`.

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.

- Убедитесь, что DNS-сервер в сети.

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

Чтобы установить Kaspersky Security Center, 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. Прочтите Лицензионное соглашение 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.

   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 DNS-имя или 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 не может содержать менее 8 или более 16 символов.
   - Пароль должен содержать символы как минимум трех групп списка ниже:
     - верхний регистр (A–Z);
     - нижний регистр (a–z);
     - 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 Linux 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.

Чтобы установить Kaspersky Security Center в тихом режиме:

1. Прочитайте Лицензионное соглашение. 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 14 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.

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

Имя переменной	Обязательная	Описание	Возможные значения
EULA_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Лицензионного соглашения.	1
PP_ACCEPTED	Да	Подтверждает, что вы понимаете и принимаете условия Политики конфиденциальности.	1
KLSRV_UNATT_SERVERADDRESS	Да	DNS-имя Сервера администрирования или статический IP-адрес.	DNS-имя устройства или IP-адрес.
KLSRV_UNATT_PORT_SRV	Нет	Номер порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 14000.	Номер порта
KLSRV_UNATT_PORT_SRV_SSL	Нет	Номер SSL-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13000.	Номер порта
KLSRV_UNATT_PORT_KLOAPI	Нет	Номер KLOAPI-порта Сервера администрирования. Необязательный параметр. По умолчанию указано значение 13299.	Номер порта
KLSRV_UNATT_PORT_GUI	Нет	Номер GUI-порта Сервера администрирования. Необязательный	Номер порта

		параметр. По умолчанию указано значение 13291.	
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_INSTANCE	Да	IP-адрес сервера базы данных.	IP-адрес;
KLSRV_UNATT_DBMS_PORT	Да	Порт сервера базы данных.	3306
KLSRV_UNATT_DB_NAME	Да	Имя базы данных.	kav
KLSRV_UNATT_DBMS_LOGIN	Да	Имя пользователя, имеющего доступ к базе данных.	
KLSRV_UNATT_DBMS_PASSWORD	Да	Пароль пользователя, который имеет доступ к базе данных.	
KLSRV_UNATT_KLADMINSGROUP	Да	Имя группы безопасности для служб.	kladmins
KLSRV_UNATT_KLSRVUSER	Да	Имя учетной записи для запуска службы Сервера администрирования. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Да	Имя учетной записи для запуска других служб. Учетная запись должна быть членом группы безопасности, указанной в переменной KLSRV_UNATT_KLADMINSGROUP.	ksc

Если Сервер администрирования будет развернут как отказоустойчивый кластер Kaspersky Security Center, 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:

KLFOC_UNATT_CONN_MODE_VA_NAME	Да	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 систему управления базами данных.
- Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux.
- Загрузите ключ программы 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) 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 программы:

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

4. Поместите ключ программы в директорию, созданную на предыдущем шаге:

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

5. Обновите оперативную память дисков:

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

   Перезагрузите систему.

6. 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. Прочтите Лицензионное соглашение 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 16.
- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A–Z);
  - нижний регистр (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 14 Web Console

В этом разделе описано, как установить Сервер Kaspersky Security Center 14 Web Console (далее также Kaspersky Security Center 14 Web Console) на устройства с операционными системами Linux. Сначала необходимо установить СУБД и Сервер администрирования Kaspersky Security Center.

Используйте один из следующих установочных файлов, соответствующих дистрибутиву Linux, установленному на вашем устройстве:

- Для Debian: ksc-web-console-[номер_сборки].x86_64.deb.
- Для операционных систем на базе RPM: ksc-web-console-[номер_сборки].x86_64.rpm.
- Для Альт 8 СП: ksc-web-console-[номер_сборки]-alt8p.x86_64.rpm.

Вы получите установочный файл, загрузив его с сайта "Лаборатории Касперского".

Чтобы установить Kaspersky Security Center 14 Web Console:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center 14 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". Если вы не согласны с условиями Лицензионного соглашения, не устанавливайте программу.
3. Создайте файл ответов, который содержит параметры для подключения Kaspersky Security Center 14 Web Console к Серверу администрирования. Назовите этот файл ksc-web-console-setup.json и расположите его в следующей директории: /etc/ksc-web-console-setup.json.

   Пример файла ответов, содержащего минимальный набор параметров, адрес и порт по умолчанию:

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
     "acceptEula": true
   }
   ```

   Рекомендуется указывать номера портов больше 1024. Если вы хотите, чтобы программа Kaspersky Security Center 14 Web Console работала на портах ниже 1024, после установки вам нужно выполнить следующую команду:

   ```
   sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
   ```

   При установке Kaspersky Security Center 14 Web Console на устройство с операционной системой ALT Linux необходимо указать номер порта, отличный от 8080, так как порт 8080 используется операционной системой.

   Программа Kaspersky Security Center 14 Web Console не может быть обновлена с помощью того же установочного файла .rpm. Если вы хотите изменить параметры файла ответов и использовать этот файл для переустановки программы, вы должны сначала удалить программу, а затем установить ее снова с новым файлом ответов.

4. Под учетной записью с привилегиями root используйте командную строку для запуска установочного файла с расширением .deb или .rpm, в зависимости от вашего дистрибутива Linux.

   - Чтобы установить или обновить предыдущую версию Kaspersky Security Center 14 Web Console из файла .deb, выполните следующую команду:

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

   - Чтобы установить Kaspersky Security Center 14 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 14 Web Console, выполните одну из следующих команд:

     - Для устройств с операционными системами RPM:

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

     - Для устройств с операционными системами Debian:

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

   Начнется распаковка установочного файла. Пожалуйста, дождитесь завершения установки. Kaspersky Security Center 14 Web Console устанавливается в следующую директорию: /var/opt/kaspersky/ksc-web-console.

5. Перезапустите все службы Kaspersky Security Center 14 Web Console, выполнив следующую команду:

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

После завершения установки вы можете использовать браузер, чтобы открыть Kaspersky Security Center 14 Web Console и осуществить вход.

Параметры установки Kaspersky Security Center 14 Web Console

Для установки Сервера Kaspersky Security Center 14 Web Console на устройства с операционными системами Linux необходимо создать файл ответов (файл .json), который содержит параметры подключения Kaspersky Security Center 14 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|Сервер администрирования  KSC",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Группа1 : Пользователь1",
  "managementServiceAccount": "Группа1 : Пользователь2",
  "serviceWebConsoleAccount": "Группа1 : Пользователь3",
  "pluginAccount": "Группа1 : Пользователь4",
  "messageQueueAccount": "Группа1 : Пользователь5"
}
```

Рекомендуется указывать номера портов больше 1024. Если вы хотите, чтобы программа Kaspersky Security Center 14 Web Console работала на портах ниже 1024, после установки вам нужно выполнить следующую команду:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

При установке Kaspersky Security Center 14 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.

Параметры установки Kaspersky Security Center 14 Web Console на устройствах с операционными системами Linux

Параметр	Описание	Доступные значения
`address`	Адрес Сервера Kaspersky Security Center 14 Web Console (обязательный параметр).	Строковое значение.
`port`	Номер порта, который Сервер Kaspersky Security Center 14 Web Console использует для подключения к Серверу администрирования (обязательный параметр).	Числовое значение.
`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 14 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 14 Web Console. Для каждого Сервера администрирования должны быть заданы следующие параметры: • адрес Сервера администрирования; • порт OpenAPI, который используется программой Kaspersky Security Center 14 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 "`.
`acceptEula`	Принимаете ли вы условия Лицензионного соглашения. Файл, содержащий условия Лицензионного соглашения, загружается вместе с установочным файлом.	Логическое значение: • `true` – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия и положения настоящего Лицензионного соглашения. • `false` – Я не принимаю условия Лицензионного соглашения (выбрано по умолчанию). Если значение не указано, программа установки Kaspersky Security Center 14 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`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console.	Строковое значение следующего формата: `" group name : user name "`.

		Например: `" Group1 : User1 "`. Если значение не указано, установщик Kaspersky Security Center 14 Web Console создает по умолчанию учетную запись `user_management_%uid%`.
`managementServiceAccount`	Имя привилегированной учетной записи, под которой запущена служба Kaspersky Security Center Web Console Management Service.	Строковое значение следующего формата: `" group name : user name "`. Например: `" Group1 : User1 "`. Если значение не указано, установщик Kaspersky Security Center 14 Web Console создает по умолчанию учетную запись `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console.	Строковое значение следующего формата: `" group name : user name "`. Например: `" Group1 : User1 "`. Если значение не указано, установщик Kaspersky Security Center 14 Web Console создает по умолчанию учетную запись `user_svc_nodejs_%uid%`.
`pluginAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Product Plugins.	Строковое значение следующего формата: `" group name : user name "`. Например: `" Group1 : User1 "`. Если значение не указано, установщик Kaspersky Security Center 14 Web Console создает по умолчанию учетную запись `user_web_plugin_%uid%`.
`messageQueueAccount`	Имя учетной записи, под которой запущена служба Kaspersky Security Center Web Console Message Queue.	Строковое значение следующего формата: `" group name : user name "`. Например: `" Group1 : User1 "`. Если значение не указано, установщик Kaspersky Security Center 14 Web Console создает по умолчанию учетную запись `user_message_queue_%uid%`.

Если вы указываете параметры `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` или `messageQueueAccount`, убедитесь, что настраиваемые учетные записи пользователей принадлежат к одной и той же группе безопасности. Если эти параметры не указаны, установщик Kaspersky Security Center 14 Web Console создает группу безопасности по умолчанию, а затем создает в этой группе учетные записи пользователей с именами по умолчанию.

Установка Kaspersky Security Center 14 Web Console, подключенной к Серверу администрирования, установленного на узлах отказоустойчивого кластера Kaspersky Security Center Linux

В этом разделе описывается установка Сервера Kaspersky Security Center 14 Web Console (далее также Kaspersky Security Center 14 Web Console), который подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера Kaspersky Security Center Linux. Перед установкой Kaspersky Security Center 14 Web Console установите СУБД и Сервер администрирования Kaspersky Security Center на узлы отказоустойчивого кластера Kaspersky Security Center Linux.

Чтобы установить Kaspersky Security Center 14 Web Console, которая подключается к Серверу администрирования, установленному на узлах отказоустойчивого кластера Kaspersky Security Center Linux:

1. Выполните шаг 1 и шаг 2 из раздела Установка Kaspersky Security Center 14 Web Console.
2. На шаге 3 в файле ответов, укажите `доверенный` параметр установки, разрешающий отказоустойчивому кластеру Kaspersky Security Center Linux подключаться к Kaspersky Security Center 14 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 Linux. В противном случае укажите IP-адрес стороннего балансировщика нагрузки, который вы используете.
   - **Порт Сервера администрирования**. Порт OpenAPI, который Kaspersky Security Center 14 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 Linux. Путь по умолчанию к файлу сертификата: <shared data folder>\1093\cert\klserver.cer. Скопируйте файл сертификата из общего хранилища данных на устройство, на котором вы устанавливаете Kaspersky Security Center 14 Web Console. Укажите локальный путь к сертификату Сервера администрирования.

- **Имя Сервера администрирования**. Имя отказоустойчивого кластера Kaspersky Security Center Linux, которое будет отображаться в окне входа в Kaspersky Security Center 14 Web Console.

3. Продолжите стандартную установку Kaspersky Security Center 14 Web Console.

После завершения установки на рабочем столе появляется ярлык и вы можете войти в Kaspersky Security Center 14 Web Console.

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

Установка Агента администрирования для Linux в тихом режиме (с файлом ответов)

Вы можете установить Агент администрирования на устройства с операционной системой Linux с помощью файла ответов – текстового файла, который содержит пользовательский набор параметров установки: переменные и их соответствующие значения. Использование файла ответов позволяет запустить установку в тихом режиме, то есть без участия пользователя.

Чтобы выполнить установку Агента администрирования для Linux в тихом режиме:

1. Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

2. Прочитайте Лицензионное соглашение. Следуйте шагам ниже, только если вы понимаете и принимаете условия Лицензионного соглашения.

3. Задайте значение переменной среды KLAUTOANSWERS, введя полное имя файла ответов (включая путь), например, следующим образом:

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

4. Создайте файл ответов (в формате TXT) в каталоге, который вы указали в переменной среды. Добавьте в файл ответов список переменных в формате VARIABLE_NAME = variable_value, каждая переменная находится на отдельной строке.

   Для правильного использования файла ответов вы должны включить в него минимальный набор из трех обязательных переменных:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Вы также можете добавить любые дополнительные переменные, чтобы использовать более конкретные параметры вашей удаленной установки. В следующей таблице перечислены все переменные, которые можно включать в файл ответов:

   Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

   Переменные файла ответов, используемые в качестве параметров установки Агента администрирования для Linux в тихом режиме

Имя переменной	Обязательная	Описание	Возможные значения
KLNAGENT_SERVER	Да	Содержит имя Сервера администрирования, представленное как полное доменное имя (FQDN) или IP-адрес.	DNS-имя устройства или IP-адрес.
KLNAGENT_AUTOINSTALL	Да	Определяет, включен ли тихий режим установки.	1 – тихий режим включен; пользователю не предлагается никаких действий во время установки. Другое – тихий режим выключен; пользователю могут быть предложены действия во время установки.
EULA_ACCEPTED	Да	Определяет, принимает ли пользователь Лицензионное соглашение Агента администрирования; если переменная не указана это может быть истолковано как отклонение Лицензионного соглашения.	1 – Я подтверждаю, что полностью прочитал(а), понимаю и принимаю условия Лицензионного соглашения. Другое значение или не задано – Я не согласен с условиями Лицензионного соглашения (установка не выполняется).
KLNAGENT_PROXY_USE	Нет	Определяет, будет ли соединение с Сервером администрирования использовать параметры прокси-сервера. По умолчанию указано значение 0.	1 – используются параметры прокси-сервера. Другое – параметра прокси-сервера не используются.

KLNAGENT_PROXY_ADDR	Нет	Определяет адрес прокси-сервера, используемого для соединения с Сервером администрирования.	DNS-имя устройства или IP-адрес.
KLNAGENT_PROXY_LOGIN	Нет	Определяет имя пользователя, используемое для входа на прокси-сервер.	Любое существующее имя пользователя.
KLNAGENT_PROXY_PASSWORD	Нет	Определяет пароль пользователя, используемый для входа на прокси-сервер.	Любой набор букв и цифр, разрешенных форматом пароля в операционной системе.
KLNAGENT_VM_VDI	Нет	Определяет, установлен ли Агент администрирования на образ для создания динамических виртуальных машин.	1 – Агент администрирования установлен на образ, который затем будет использован для создания динамических виртуальных машин. Другое – во время установки образ не используется.
KLNAGENT_VM_OPTIMIZE	Нет	Определяет, являются ли параметры Агента администрирования оптимальными для гипервизора.	1 – локальные параметры Агента администрирования по умолчанию изменены таким образом, что они позволяют оптимизировать использование на гипервизоре.
KLNAGENT_TAGS	Нет	Перечисляет теги, назначенные экземпляру Агента администрирования.	Один или несколько тегов, разделенных точкой с запятой.
KLNAGENT_UDP_PORT	Нет	Определяет UDP-порт, используемый Агентом администрирования. По умолчанию указано значение 15000.	Любой существующий номер порта.
KLNAGENT_PORT	Нет	Определяет порт (не TLS), используемый Агентом администрирования. По умолчанию указано значение 14000.	Любой существующий номер порта.
KLNAGENT_SSLPORT	Нет	Определяет TLS-порт, используемый Агентом администрирования. По умолчанию указано значение 13000.	Любой существующий номер порта.
KLNAGENT_USESSL	Нет	Определяет, используется ли безопасность транспортного уровня (TLS) для подключения.	1 (по умолчанию) – используется TLS. Другое – TLS не используется.
KLNAGENT_GW_MODE	Нет	Определяет, используется ли шлюз соединения.	1 (по умолчанию) – текущие параметры не изменяются (при первом вызове шлюз соединения не указывается). 2 – шлюз соединения не используется. 3 – используется шлюз соединения. KLNAGENT_GW_ADDRESS – обязательный параметр. 4 – экземпляр Агента администрирования используется в качестве шлюза соединения в демилитаризованной зоне (DMZ). Требуется сертификат Сервера.
KLNAGENT_GW_ADDRESS	Нет	Определяет адрес шлюза соединения. Значение применимо, только если KLNAGENT_GW_MODE = 3.	DNS-имя устройства или IP-адрес.

5. Установка Агента администрирования:

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
  `# rpm -i klnagent-<номер сборки>.i386.rpm`

- Чтобы установить Агент администрирования из RPM-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
  `# rpm -i klnagent64-<номер сборки>.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-<номер сборки>.aarch64.rpm`

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent_<номер сборки>_i386.deb`

- Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<номер сборки>_amd64.deb`

- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  `# apt-get install ./klnagent64_<номер сборки>_arm64.deb`

Установка Агента администрирования для Linux начинается в тихом режиме; пользователю не предлагается выполнять никаких действий во время процесса.

Установка Агента администрирования на Astra Linux в режиме замкнутой программной среды

В этом разделе описывается, как установить Агент администрирования для Linux на устройство с операционной системой Astra Linux Special Edition.

Перед установкой:

- Убедитесь, что на устройстве, на которое вы хотите установить Агент администрирования Linux, работает один из поддерживаемых дистрибутивов Linux.
- Загрузите ключ программы kaspersky_astra_pub_key.gpg.
- Загрузите установочный файл Агента администрирования с сайта "Лаборатории Касперского".

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

Чтобы установить Агент администрирования для Linux на устройство с операционной системой Astra Linux Special Edition (обновление 1.7) 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 программы:
   `mkdir -p /etc/digsig/keys/legacy/kaspersky/`
4. Поместите ключ программы в директорию, созданную на предыдущем шаге:
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`
5. Обновите оперативную память дисков:
   `update-initramfs -u -k all`
   Перезагрузите систему.
6. Установка Агента администрирования:

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 32-разрядной операционной системой, выполните следующую команду:
     `# apt-get install ./klnagent_<номер сборки>_i386.deb`

   - Чтобы установить Агент администрирования из DEB-пакета на устройство с 64-разрядной операционной системой, выполните следующую команду:

```
# apt-get install ./klnagent64_<номер сборки>_amd64.deb
```

- Чтобы установить Агент администрирования из DEB-пакета на устройство архитектуры ARM с 64-разрядной операционной системой, выполните следующую команду:
  ```
  # apt-get install ./klnagent64_<номер сборки>_arm64.deb
  ```

Агент администрирования для Linux установлен.

Учетная запись для работы с СУБД

Для установки Сервера администрирования и работы с ним требуется создать внутреннюю учетную запись СУБД. Эта учетная запись позволяет вам получить доступ к СУБД. Для такой учетной записи требуются определенные права. Когда вы предоставляете права и разрешения учетной записи СУБД, следуйте принципу наименьших привилегий. Это означает, что предоставленных прав достаточно только для выполнения требуемых действий. Обратите внимание, что вам нужно предоставить права учетной записи СУБД перед установкой и запуском Сервера администрирования.

Kaspersky Security Center 14 Linux поддерживает СУБД MySQL и MariaDB. После создания внутренней учетной записи для одной из этих СУБД, предоставьте этой учетной записи необходимые права. Обратите внимание, что наборы прав для внутренней учетной записи MySQL и внутренней учетной записи MariaDB одинаковы. 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.

Прав, которые вы предоставили для внутренней учетной записи СУБД, достаточно для восстановления данных Сервера администрирования из резервной копии.

Настройка учетной записи СУБД для работы с MySQL и MariaDB

Предварительные требования

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

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

Настройка учетной записи СУБД для установки Сервера администрирования

Чтобы настроить учетную запись СУБД для установки Сервера администрирования:

1. Запустите среду для работы с MySQL или MariaDB под учетной записью root, которую вы создали при установке СУБД.
2. Создайте внутреннюю учетную запись СУБД с паролем. Программа установки Сервера администрирования (далее также программа установки) и служба Сервера администрирования используют эту внутреннюю учетную запись СУБД для доступа к СУБД.

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

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

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

   - Чтобы создать учетную запись СУБД, использующую "Собственный пароль MySQL", выполните следующую команду:
     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<пароль>';
     ```
   - Чтобы изменить аутентификацию для существующей учетной записи СУБД, выполните следующую команду:
     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<пароль>';
     ```
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 ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

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

6. Установите Сервер администрирования.

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

Развертывание отказоустойчивого кластера Kaspersky Security Center Linux

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

Сценарий: Развертывание отказоустойчивого кластера Kaspersky Security Center Linux

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.

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

1. **Создание учетных записей для служб Kaspersky Security Center**

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

   1. Создайте доменную 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.

2. **Подготовка файлового сервера**

Подготовьте файловый сервер к работе в составе отказоустойчивого кластера Kaspersky Security Center Linux. 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 Linux.

3. **Подготовка активного и пассивного узлов**

   Подготовьте два компьютера с идентичным аппаратным и программным обеспечением для работы в качестве активного и пассивного узлов.

   Инструкции: Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center Linux.

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

   У вас есть два варианта:

   - Если вы хотите использовать MariaDB Galera Cluster, выделенный компьютер для СУБД не требуется. Установите кластер MariaDB Galera на каждый из узлов.
   - Если вы хотите использовать любую другую поддерживаемую СУБД, установите выбранную СУБД на выделенный компьютер.

5. **Установка Kaspersky Security Center**

   Установите Kaspersky Security Center в режиме отказоустойчивого кластера на оба узла. Сначала необходимо установить Kaspersky Security Center на активный узел, а затем установить его на пассивный.

   Также вы можете установить Kaspersky Security Center 14 Web Console на отдельном устройстве, не являющемся узлом кластера.

6. **Тестирование отказоустойчивого кластера**

   Убедитесь, что вы правильно настроили отказоустойчивый кластер и правильно ли он работает. Например, вы можете остановить одну из служб Kaspersky Security Center на активном узле: kladminserver, klnagent, ksnproxy, klactprx или klwebsrv. После остановки службы управление защитой должно быть автоматически переключено на пассивный узел.

Результаты

Отказоустойчивый кластер Kaspersky Security Center Linux развернут. Пожалуйста, ознакомьтесь с событиями, которые приводят к переключению между активными и пассивными узлами.

Об отказоустойчивом кластере Kaspersky Security Center Linux

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

Аппаратные и программные требования

Для развертывания отказоустойчивого кластера Kaspersky Security Center Linux у вас должно быть следующее оборудование:

- Два устройства с одинаковым аппаратным и программным обеспечением. Эти устройства будут использоваться как активный и пассивный узлы.
- Файловый сервер под управлением Linux с файловой системой EXT4. Вам нужно выделить отдельное устройство, которое будет выступать в качестве файлового сервера.

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

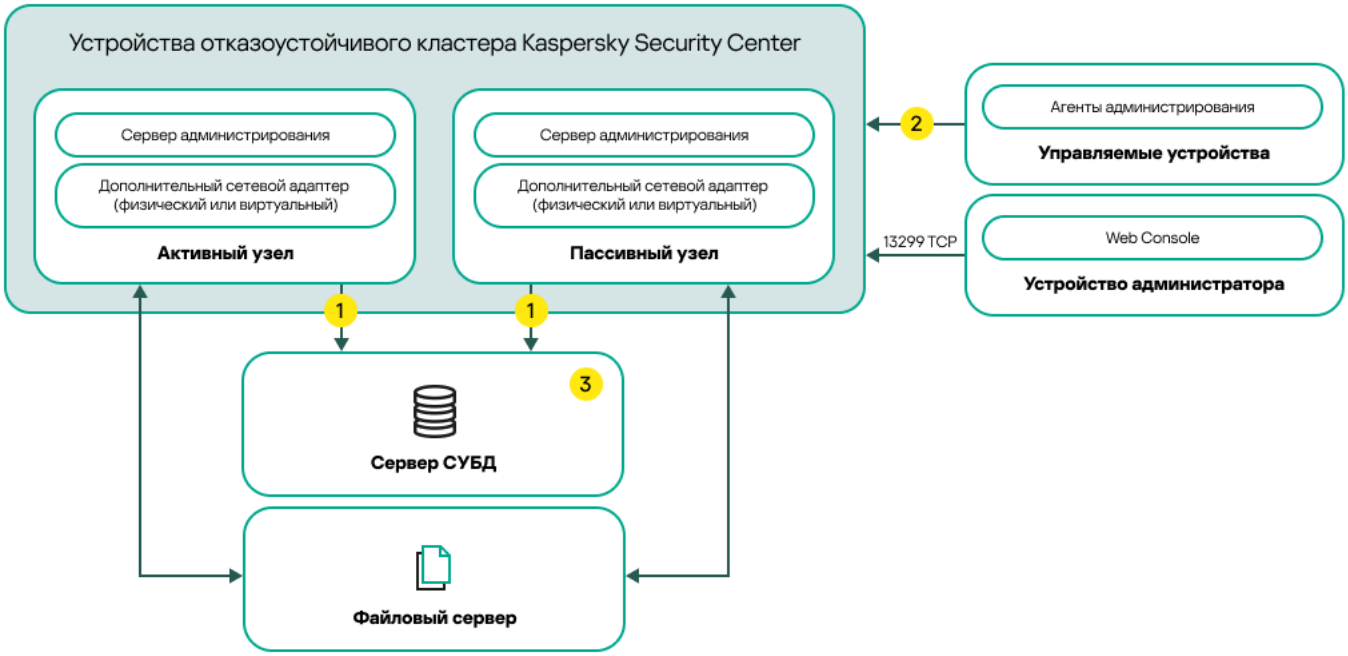
- Устройство с поддерживаемой системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, отдельное устройство для этой цели не требуется.

Не удается выполнить развертывание отказоустойчивого кластера, если у вас установлены либо оба пакета arping и iputils-arping, либо только пакет arping. Перед развертыванием отказоустойчивого кластера убедитесь, что на обоих узлах установлен только инсталляционный пакет iputils-arping.

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.



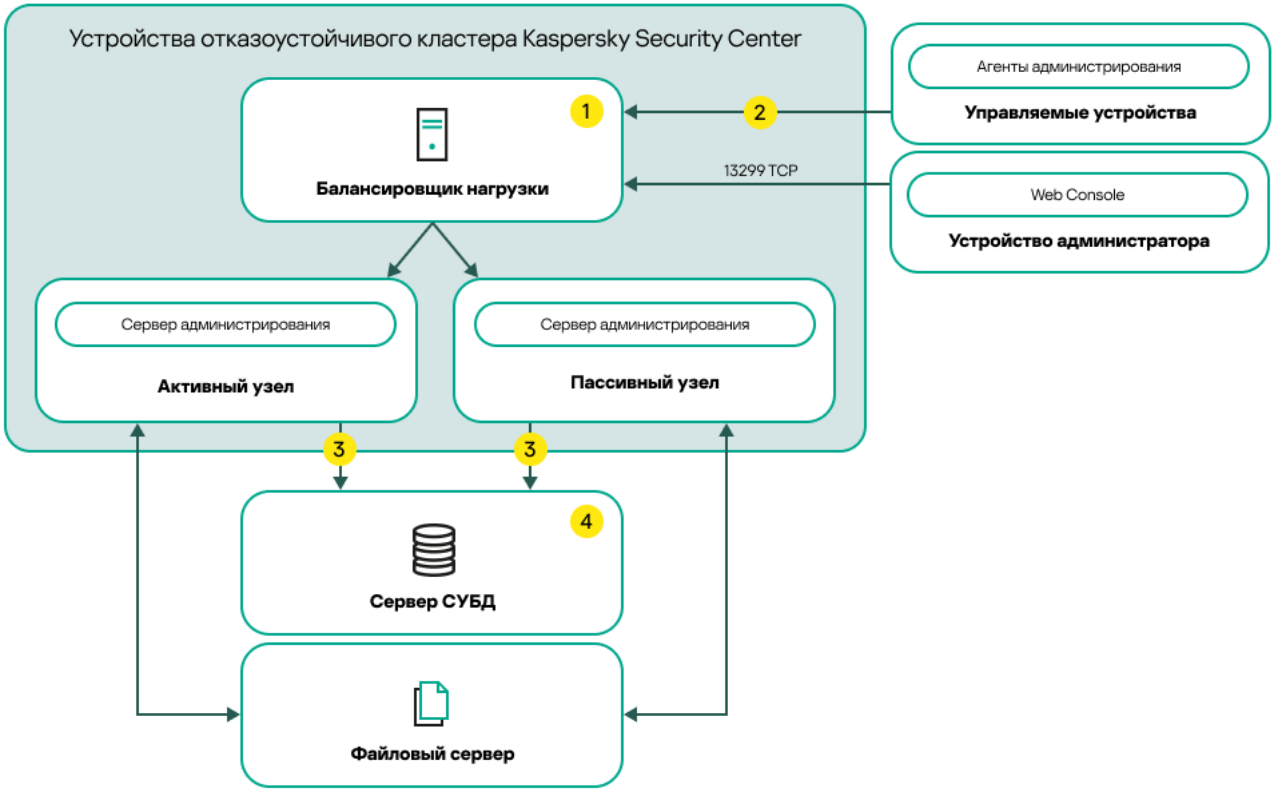
Схема, в которой используется дополнительный сетевой адаптер

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 5432 для PostgreSQL или Postgres Pro. Подробную информацию см. в документации СУБД.

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

3 Устройство с системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, отдельное устройство 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 13299 и TCP 17000.

> Если вы хотите использовать утилиту klakaut для автоматизации, вам также необходимо открыть TCP-порт 13291.

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 5432 для PostgreSQL или Postgres Pro. Подробную информацию см. в документации СУБД.

4 Устройство с системой управления базами данных (СУБД). Если вы используете MariaDB Galera Cluster в качестве СУБД, отдельное устройство 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.
- 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 Linux

Файловый сервер работает как обязательный компонент отказоустойчивого кластера Kaspersky Security Center Linux.

Чтобы подготовить файловый сервер:

1. Убедитесь, что файловый сервер соответствует аппаратным и программным требованиям.
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.

   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 *\(rw,sync,no_subtree_check,no_root_squash\) >> /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 Linux, следуйте инструкциям этого сценария.

Подготовка узлов для отказоустойчивого кластера Kaspersky Security Center Linux

Подготовьте два компьютера к работе в качестве активного и пассивного узла для отказоустойчивого кластера Kaspersky Security Center Linux.

Чтобы подготовить узлы для отказоустойчивого кластера Kaspersky Security Center Linux:

1. Убедитесь, что у вас есть два компьютера, соответствующих аппаратным и программным требованиям. 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,auto,user,rw {сервер}:{путь к папке KlFocStateShare folder} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,noauto,user,rw {сервер}:{путь к папке KlFocDataShare_klfoc folder}
   /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 folder} /mnt/KlFocStateShare nfs
   vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0
   {сервер}:{путь к папке KlFocDataShare_klfoc folder} /mnt/KlFocDataShare_klfoc nfs vers=4,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 стандартными средствами операционной системы. Если вы хотите использовать виртуальный сетевой адаптер, создайте его с помощью программ сторонних производителей

   Выполните одно из следующих действий:

   - Используйте виртуальный сетевой адаптер.

     a. Введите следующую команду, чтобы убедиться, что NetworkManager используется для управления физическим адаптером:
     ```
     nmcli device status
     ```

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

     b. Используйте следующую команду для идентификации интерфейсов:
     ```
     ip a
     ```

c. Создайте профиль конфигурации:

```
nmcli connection add type macvlan dev <физический интерфейс> mode bridge ifname <виртуальный интерфейс> ipv4.addresses <маска 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 13299 и TCP 17000.

  > Если вы хотите использовать утилиту klakaut для автоматизации, вам также необходимо открыть TCP-порт 13291.

Узлы подготовлены. Чтобы развернуть отказоустойчивый кластер Kaspersky Security Center Linux, следуйте инструкциям сценария.

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. Kaspersky Security Center устанавливается на оба узла отказоустойчивого кластера Kaspersky Security Center по отдельности. Сначала вы устанавливаете программу на активный узел, затем на пассивный. Во время установки вы выбираете, какой узел будет активным, а какой пассивным.

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

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

Установка на основной (активный) узел

Чтобы установить Kaspersky Security Center на основном узле:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux.
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. Прочтите Лицензионное соглашение 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 порта Сервера администрирования. По умолчанию номер порта – 14000.

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

h. 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.

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

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

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

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

m. Введите номер порта базы данных. Этот порт используется для связи с Сервером администрирования. По умолчанию номер порта – 3306.

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:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc

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

Пользователь добавлен, и Kaspersky Security Center установлен первичном узле.

Установка на вторичном (пассивном) узле

Чтобы установить Kaspersky Security Center на вторичный узел:

1. Убедитесь, что на устройстве, на которое вы хотите установить Kaspersky Security Center, работает один из поддерживаемых дистрибутивов Linux.
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. Прочтите Лицензионное соглашение и Политику конфиденциальности. Текст отображается в окне командной строки. Нажмите пробел, чтобы просмотреть следующий фрагмент текста. При отображении запроса введите следующие значения:
   a. Введите `y`, если вы понимаете и принимаете условия Лицензионного соглашения. Введите `n`, если вы не принимаете условия Лицензионного соглашения. Чтобы использовать Kaspersky Security Center, вы должны принять условия Лицензионного соглашения.
   b. Введите `y`, если вы понимаете и принимаете условия Политики конфиденциальности и соглашаетесь, что ваши данные будут обрабатываться и пересылаться (в том числе в третьи страны), согласно Политике конфиденциальности. Введите `n`, если вы не принимаете условия Политики конфиденциальности. Чтобы использовать Kaspersky Security Center, вы должны принять условия Политики конфиденциальности.
6. Выберите **Вторичный узел кластера** как режим установки Сервера администрирования.
7. При появлении запроса введите локальный путь к точке подключения общей папки состояния.

Программа Kaspersky Security Center установлена на вторичном узле.

Проверка служб

Используйте следующие команды, чтобы проверить, запущена ли служба:

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

Теперь вы можете протестировать отказоустойчивый кластер 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 Linux 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.

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.

О сертификатах Kaspersky Security Center

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

- сертификат Сервера администрирования;
- мобильный сертификат;
- сертификат Веб-сервера;
- сертификат Kaspersky Security Center 14 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 14 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;
- M – мобильный сертификат для порта 13292;
- MR – мобильный резервный сертификат для порта 13292;
- MCA – мобильный сертификат, полученный от доверенного центра сертификации для автоматической генерации пользовательских сертификатов.

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

Сертификаты Сервера администрирования

Сертификат Сервера администрирования необходим для следующих целей:

- аутентификации Сервера администрирования при подключении к Kaspersky Security Center 14 Web Console;
- безопасного взаимодействия Сервера администрирования и Агента администрирования на управляемых устройствах;

- аутентификации 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 14 Web Console. 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.

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

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.

Если вы открываете Kaspersky Security Center 14 Web Console в разных браузерах и загружаете файл сертификата Сервера администрирования в окне свойств Сервера администрирования, загруженные файлы имеют разные имена.

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.

Также сертификат Сервера iOS MDM необходим для аутентификации Сервера администрирования на мобильных устройствах под управлением операционной системы iOS. Подробнее см. раздел Настройка сертификата Сервера iOS MDM.

Сертификат Веб-сервера

Веб-сервер является компонентом Сервера администрирования Kaspersky Security Center и использует специальный тип сертификата. Этот сертификат необходим для публикации инсталляционных пакетов Агента администрирования, которые вы впоследствии загружаете на управляемые устройства, а также для инсталляционных пакетов Kaspersky Security для мобильных устройств. Для этого Веб-сервер может использовать различные сертификаты.

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

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

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

1. Пользовательский сертификат Веб-сервера, который вы указали вручную с помощью Консоли администрирования.
2. Пользовательский мобильный сертификат.

3. Самоподписанный мобильный сертификат ("M").

4. Общий сертификат Сервера администрирования ("C").

сертификат Kaspersky Security Center 14 Web Console.

Сервер Kaspersky Security Center 14 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 на пользовательский сертификат (рекомендуемый параметр). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
- Добавить сертификат Web Console в список доверенных сертификатов браузера. Рекомендуется использовать этот параметр только в том случае, если вы не можете создать пользовательский сертификат.

Требования к пользовательским сертификатам, используемым в Kaspersky Security Center

В таблице ниже представлены требования к пользовательским сертификатам, предъявляемые к различным компонентам Kaspersky Security Center.

Требования для сертификатов Kaspersky Security Center

Тип сертификата	Требования	Комментарии
Общий сертификат, Общий резервный сертификат ("C", "CR")	Минимальная длина ключа: 2048. Основные ограничения: • Ограничение длины пути: Отсутствует. Использование ключа: • 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 поле `subjectAltName` заполнено. Сертификат соответствует действующим требованиям браузеров, предъявляемым к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	—
сертификат Kaspersky Security Center 14 Web Console.	Контейнер PEM, из которого указывается сертификат, включает всю цепочку открытых ключей. Присутствует альтернативное имя субъекта (SAN) сертификата; то есть поле `subjectAltName` заполнено. Сертификат соответствует действующим требованиям браузеров к сертификатам серверов, а также к текущим базовым требованиям CA/Browser Forum.	Зашифрованные сертификаты не поддерживаются Kaspersky Security Center 14 Web Console.

Перевыпуск сертификата для Kaspersky Security Center 14 Web Console

Большинство браузеров ограничивает срок действия сертификата. Чтобы попасть в это ограничение, срок действия сертификата в Kaspersky Security Center 14 Web Console равен 397 дням. Вы можете заменить существующий сертификат, полученный от доверенного центра сертификации (CA), при выпуске вручную нового самоподписанного сертификата. Вы также можете повторно выпустить устаревший сертификат Kaspersky Security Center 14 Web Console.

Автоматический перевыпуск сертификата для Kaspersky Security Center 14 Web Console не поддерживается. Вам необходимо вручную перевыпустить сертификат.

Если вы выбрали создать сертификат, при открытии Kaspersky Security Center 14 Web Console, браузер может информировать вас о том, что подключение к Kaspersky Security Center 14 Web Console не является приватным и что сертификат Kaspersky Security Center 14 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). Создать сертификат, доверенный в вашей инфраструктуре и соответствующий требованиям к пользовательским сертификатам.
- Добавьте сертификат Kaspersky Security Center 14 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 14 Web Console:

Переустановите Kaspersky Security Center 14 Web Console, выполнив одно из следующих действий:

- Если вы хотите использовать тот же установочный файл Kaspersky Security 14 Center Web Console, удалите Kaspersky Security Center 14 Web Console и установите ту же версию Kaspersky Security Center 14 Web Console.
- Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления.

Сертификат Kaspersky Security Center 14 Web Console перевыпущен со сроком действия 397 дней.

Замена сертификата для Kaspersky Security Center 14 Web Console

По умолчанию при установке Сервера Kaspersky Security Center 14 Web Console (далее также Kaspersky Security Center 14 Web Console Server) сертификат браузера для программы генерируется автоматически. Вы можете заменить автоматически сгенерированный сертификат на пользовательский.

Чтобы заменить сертификат для Kaspersky Security Center 14 Web Console на пользовательский сертификат:

1. Создайте новый файл ответов, необходимый для установки Kaspersky Security Center 14 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 14 Web Console, указав новый файл ответов. Выполните одно из следующих действий:
   - Если вы хотите использовать тот же установочный файл Kaspersky Security 14 Center Web Console, удалите Kaspersky Security Center 14 Web Console и установите ту же версию Kaspersky Security Center 14 Web Console.
   - Если вы хотите использовать установочный файл обновленной версии, выполните команду обновления.

Kaspersky Security Center 14 Web Console работает с указанным сертификатом.

Преобразование сертификата из формата PFX в формат PEM

Чтобы использовать сертификат формата PFX в Kaspersky Security Center 14 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 14 Web Console не поддерживает сертификаты, защищенные парольной фразой. Поэтому выполните следующую команду в кроссплатформенной утилите на основе OpenSSL, чтобы удалить парольную фразу из файла .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   Не используйте одно и то же имя для входных и выходных файлов .pem.

В результате новый файл .pem не зашифрован. Вводить парольную фразу для его использования не нужно.

Файлы .crt и .pem готовы к использованию, поэтому вы можете указать их в мастере установки Kaspersky Security Center 14 Web Console.

Сценарий: Задание пользовательского сертификата Сервера администрирования

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

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

Предварительные требования

Новый сертификат должен быть создан в формате PKCS#12 (например, с помощью PKI организации) и должен быть выпущен 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 для этой цели утилиту командной строки klsetsrvcert.

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

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

Результаты

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

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.

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 сертификат до истечения срока действия общим резервным сертификатом. Укажите время, когда управляемые устройства должны синхронизироваться с Сервером администрирования с использованием нового сертификата.
`-i <inputfile>`	Контейнер с сертификатом и закрытый ключ в формате PKCS#12 (файл с расширением p12 или pfx).
`-p <password>`	Пароль, при помощи которого защищен p12-контейнер. Сертификат и закрытый ключ хранятся в контейнере, поэтому для расшифровки файла с контейнером требуется пароль.
`-o <chkopt>`	Параметры проверки сертификата (разделенные точкой с запятой). Чтобы использовать пользовательский сертификат без разрешения на подпись, в утилите klsetsrvcert укажите `-o NoCA`. Это полезно для сертификатов, выпущенных доверенным центром сертификации (англ. certificate authority, CA). Чтобы изменить длину ключа шифрования для сертификатов типа C или CR, укажите в утилите klsetsrvcert `-o RsaKeyLen:< длина ключа >`, где параметр `< длина ключа >` – это необходимая 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:

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.

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.

Подключение Агентов администрирования к Серверу администрирования с помощью утилиты klmover

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

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.

Вы не можете использовать утилиту klmover для клиентских устройств, подключенных к Серверу администрирования через шлюзы соединения. Для таких устройств необходимо перенастроить Агент администрирования или переустановить Агент администрирования, указав шлюз соединения.

Описание параметров утилиты klmover представлено в таблице ниже.

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.

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.

Обновление предыдущей версии Kaspersky Security Center Linux

Вы можете установить Сервер администрирования версии 14 на устройство, на котором установлена предыдущая версия Сервера администрирования (начиная с версии 13). При обновлении до версии 14 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. При необходимости вы можете перенести Сервер администрирования на другое устройство с более поздними версиями операционной системы и СУБД.

Вы можете обновить версию Сервера администрирования одним из следующих способов:

- С помощью установочного файла Kaspersky Security Center.

- Создав резервную копию данных Сервера администрирования, установив новую версию Сервера администрирования и восстановив данные Сервера администрирования из резервной копии.

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

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

Также вам необходимо обновить Kaspersky Security Center 14 Web Console до новой версии.

При обновлении предыдущей версии Kaspersky Security Center Linux все установленные плагины поддерживаемых программ "Лаборатории Касперского" сохраняются. Плагины Сервера администрирования и Агента администрирования обновляются автоматически. Перед началом обновления рекомендуется создать резервную копию данных Сервера администрирования.

Обновление предыдущей версии Kaspersky Security Center Linux с помощью файла установки

Для обновления Сервера администрирования с предыдущей версии (начиная с версии 13) до версии 14 вы можете установить новую версию поверх предыдущей с помощью установочного файла Kaspersky Security Center Linux.

Чтобы обновить Сервер администрирования предыдущей версии до версии 14 с помощью установочного файла:

1. Загрузите установочный файл Kaspersky Security Center с полным пакетом для версии 14 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 программы будет продолжена после того, как вы дважды введете "Y".
5. Введите "1", чтобы выбрать стандартный режим установки Сервера администрирования.

   На картинке ниже показаны последние два шага.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Принятие условий Лицензионного соглашения и Политики конфиденциальности и выбор стандартного режима установки Сервера администрирования в терминале командной строки

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 Linux.

   После выполнения задачи удаленной установки версия Агента администрирования обновлена.

Обновление предыдущей версии Kaspersky Security Center Linux с помощью резервной копии

Для обновления Сервера администрирования с предыдущей версии (начиная с версии 13) до версии 14 вы можете создать резервную копию данных Сервера администрирования и восстановить эти данные после установки Kaspersky Security Center Linux 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 14 с помощью резервной копии данных:

1. Перед обновлением, выполните резервное копирование данных Сервера администрирования старой версии программы.
2. Удалите старую версию Kaspersky Security Center.
3. Установите Kaspersky Security Center версии 14 на бывшем Сервере администрирования.
4. Восстановите данные Сервера администрирования из резервной копии данных, созданной перед обновлением.
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 Linux.

   После выполнения задачи удаленной установки версия Агента администрирования обновлена.

Вход в программу Kaspersky Security Center 14 Web Console и выход из нее

Вы можете войти в Kaspersky Security Center 14 Web Console после установки Сервера администрирования и Kaspersky Security Center 14 Web Console. Вы должны знать веб-адрес Сервера администрирования и номер порта, указанный во время установки (по умолчанию используется порт 8080). В вашем браузере JavaScript должен быть включен.

Чтобы войти в Kaspersky Security Center 14 Web Console:

1. В браузере укажите <веб-адрес Сервера администрирования>:<номер порта>.

   Отобразится страница входа в программу.

2. Если вы добавили несколько доверенных Серверов администрирования, в списке выберите Сервер администрирования, к которому вы хотите подключиться.

   Если вы добавили только один Сервер администрирования, отображаются только поля **Имя пользователя** и **Пароль**.

3. Выполните одно из следующих действий:

   - Для входа на физический Сервер администрирования введите имя пользователя и пароль локального администратора.
   - Если на Сервере создан один или несколько виртуальных Серверов администрирования и вы хотите войти на виртуальный Сервер:

     a. Нажмите на кнопку **Дополнительные параметры**.

     b. Введите имя виртуального Сервера администрирования, которое вы указали при создании виртуального Сервера.

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

После входа в систему информационная панель отображается с языком и темой, которые вы использовали в последний раз. Вы можете перемещаться по Kaspersky Security Center 14 Web Console и использовать ее для работы с Kaspersky Security Center Linux.

Чтобы выйти из Kaspersky Security Center 14 Web Console,

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

Программа Kaspersky Security Center 14 Web Console закрыта, отображается страница входа в программу.

Мастер первоначальной настройки

Программа Kaspersky Security Center Linux позволяет настроить минимальный набор параметров, необходимых для построения централизованной системы управления, обеспечивающей защиту сети от угроз безопасности. Эта настройка выполняется в мастере первоначальной настройки. В процессе работы мастера вы можете внести в программу следующие изменения:

- Добавить файлы ключей или ввести коды активации, которые можно автоматически распространять на устройства в группах администрирования.
- Настроить рассылку по электронной почте оповещений о событиях в работе Сервера администрирования и управляемых программ (чтобы уведомление прошло успешно, на Сервере администрирования и на всех устройствах-получателях должна быть запущена служба сообщений Messenger).
- Сформировать политику защиты рабочих станций и серверов, а также задачи поиска вирусов, получения обновлений и резервного копирования данных для верхнего уровня иерархии управляемых устройств.

  Мастер первоначальной настройки создает политики только для программ, для которых еще нет созданных политик в папке **Управляемые устройства**. Мастер первоначальной настройки не создает задачи, если задачи с такими именами уже созданы для верхнего уровня иерархии управляемых устройств.

Программа автоматически предлагает запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к Серверу. Вы также можете запустить мастер первоначальной настройки вручную в любое время.

Чтобы запустить мастер первоначальной настройки вручную:

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

   Откроется окно свойств Сервера администрирования.
2. На вкладке **Общие** выберите раздел **Общие**.
3. Нажмите на кнопку **Запустить мастер первоначальной настройки**.

Мастер предложит произвести первоначальную настройку Сервера администрирования. Следуйте далее указаниям мастера. Для продолжения работы мастера нажмите на кнопку **Далее**.

Шаг 1. Указание параметров подключения к интернету

Развернуть все | Свернуть все

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 Linux и управляемых программ "Лаборатории Касперского".

Включите параметр **Использовать прокси-сервер**, если требуется использовать прокси-сервер для подключения к интернету. Если параметр включен, доступны поля ввода параметров. Настройте следующие параметры подключения к прокси-серверу:

- **Адрес**

  Адрес прокси-сервера для подключения Kaspersky Security Center Linux к интернету.
- **Номер порта**

  Номер порта, через который будет установлено прокси-подключение Kaspersky Security Center Linux.
- **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.

  Поле ввода доступно, если установлен флажок **Использовать прокси-сервер**.
- **Имя пользователя**

Учетная запись пользователя, от имени которого будет выполняться подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

- **Пароль**

  Пароль пользователя, с помощью учетной записи которого выполняется подключение к прокси-серверу (поле доступно, если установлен флажок **Аутентификация на прокси-сервере**).

  Чтобы посмотреть введенный пароль, нажмите на кнопку **Показать** и удерживайте ее необходимое вам время.

Вы можете настроить доступ в интернет позднее без запуска мастера первоначальной настройки.

Шаг 2. Выбор способа активации программы

Развернуть все | Свернуть все

Выберите один из следующих вариантов активации Kaspersky Security Center Linux:

- **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 Linux. Код активации отправляется вам на адрес электронной почты, указанный при приобретении Kaspersky Security Center.

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

  Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в разделе **Операции → Лицензирование → Лицензии "Лаборатории Касперского"** главного меню.

- **Укажите файл ключа**

  Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего программу.

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

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

  Если вы выбрали этот вариант активации программы, можно включить вариант **Автоматически распространять лицензионный ключ на управляемые устройства**.

  Если выбран этот вариант, лицензионный ключ будет распространяться на управляемые устройства автоматически.

  Если этот вариант не выбран, лицензионный ключ можно будет распространить на управляемые устройства позже, в разделе **Операции → Лицензирование → Лицензии "Лаборатории Касперского"** главного меню.

- Отложите активацию программы

Если вы отложили активацию программы, вы можете добавить ключ позже в любое время, выбрав **Операции → Лицензирование**.

При работе с Kaspersky Security Center, развернутым из платного образа AMI или с использованием ежемесячных счетов за использование SKU, вы не можете указать файл ключа или ввести код активации.

Шаг 3. Создание базовой конфигурации защиты сети

Вы можете проверить список созданных политик и задач.

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

Шаг 4. Настройка параметров отправки уведомлений по электронной почте

Развернуть все | Свернуть все

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

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

- **Получатели (адреса электронной почты)**

  Адреса электронной почты пользователей, которым программа будет отправлять уведомления. Вы можете указать один или более адресов. Если вы указываете несколько адресов, разделяйте их точкой с запятой.

- **Адрес SMTP-сервера**

  Адрес или адреса почтовых серверов вашей организации.

  Если вы указываете несколько адресов, разделяйте их точкой с запятой. Вы можете использовать следующие значения параметра:

  - IPv4-адрес или IPv6-адрес;
  - DNS-имя SMTP-сервера.

- **Порт SMTP-сервера**

  Номер коммуникационного порта SMTP-сервера. Если вы используете несколько SMTP-серверов, соединение с ними устанавливается через указанный коммуникационный порт. По умолчанию установлен порт 25.

- **Использовать ESMTP-аутентификацию**

  Включение поддержки ESMTP-аутентификации. После установки флажка можно указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию флажок снят.

Вы можете проверить параметры уведомления о сообщениях электронной почты с помощью кнопки **Отправить тестовое сообщение**.

Шаг 5. Завершение работы мастера первоначальной настройки

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

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

Мастер развертывания защиты

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

Мастер развертывания защиты выполнит следующие действия:

- Загружает инсталляционный пакет для установки программы (если он не был создан раньше). Инсталляционный пакет расположен: **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Инсталляционные пакеты**. Вы можете использовать этот инсталляционный пакет для установки программы в дальнейшем.
- Создает и запускает задачу удаленной установки для набора устройств или для группы администрирования. Созданная задача удаленной установки хранится в разделе **Задачи**. Вы можете запустить эту задачу в дальнейшем вручную. Тип задачи – **Удаленная установка программы**.

Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

Шаг 1. Запуск мастера развертывания защиты

Мастер развертывания защиты можно запустить вручную.

Чтобы запустить мастер развертывания защиты вручную,

В главном меню перейдите в раздел **Обнаружение устройств и развертывание** → **Развертывание и назначение** → **Мастер развертывания защиты**.

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

Шаг 2. Выбор инсталляционного пакета

Выберите инсталляционный пакет программы, которую требуется установить.

Если инсталляционный пакет требуемой программы не содержится в списке, нажмите на кнопку **Добавить** и выберите программу из списка.

Шаг 3. Выбор способа распространения файла ключа или кода активации

Развернуть все | Свернуть все

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.

Шаг 4. Выбор версии Агента администрирования

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

Выберите последнюю версию Агента администрирования.

Шаг 5. Выбор устройств

Развернуть все | Свернуть все

Укажите список устройств, на которые требуется установить программу:

- **Установить на управляемые устройства**

  Если выбран этот вариант, задача удаленной установки программы будет создана для группы устройств.

- **Выбор устройств для установки**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

Шаг 6. Задание параметров задачи удаленной установки

Развернуть все | Свернуть все

В окне **Параметры задачи удаленной установки** настройте параметры удаленной установки программы.

В блоке параметров **Принудительно загрузить инсталляционный пакет** выберите способ доставки на клиентские устройства файлов, необходимых для установки программы:

- **С помощью Агента администрирования**

  Если этот параметр включен, доставку инсталляционных пакетов на клиентские устройства выполняет установленный на клиентских устройствах Агент администрирования.

  Если этот параметр выключен, инсталляционные пакеты доставляются с помощью инструментов операционной системы клиентского устройства.

Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

По умолчанию параметр включен.

- **Средствами операционной системы с помощью точек распространения**

  Если этот параметр включен, инсталляционные пакеты передаются на клиентские устройства средствами операционной системы через точки распространения. Этот вариант можно выбрать, если в сети есть хотя бы одна точка распространения.

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

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

Настройте дополнительный параметр:

Не устанавливать программу, если она уже установлена

Если этот параметр включен, выбранная программа не устанавливается заново, если она уже установлена на клиентском устройстве.

Если этот параметр выключен, программа будет установлена в любом случае.

По умолчанию параметр включен.

Шаг 7. Удаление несовместимых программ перед установкой

Этот шаг присутствует, только если программа, которую вы разворачиваете, несовместима с другими программами.

Выберите этот параметр, если вы хотите, чтобы программа Kaspersky Security Center Linux автоматически удаляла несовместимые программы с программой, которую вы устанавливаете.

Отображается список несовместимых программ.

Если этот параметр не выбран, программа будет установлена только на устройствах, на которых нет несовместимых программ.

Шаг 8. Перемещение устройств в папку Управляемые устройства

Развернуть все | Свернуть все

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.

- **Перемещать 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

Развернуть все | Свернуть все

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

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

Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу удаленной установки. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для установки программы.

  - **Локальная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор программы. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите 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.

  - **SSH сертификат**. Если вы хотите установить программу на клиентское устройство под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

    Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Kaspersky Security Center поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen. Например:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< электронная почта пользователя >"
    ```

Шаг 10. Запуск установки

Это последний шаг мастера. На этом шаге **Задача удаленной установки программы** была успешно создана и настроена.

По умолчанию вариант **Запустить задачу после завершения работы мастера** не выбран. Если вы выберете этот параметр, **Задача удаленной установки программы** начнется сразу после завершения работы мастера. Если вы не выберете этот параметр, **Задача удаленной установки программы** не начнется. Вы можете запустить эту задачу в дальнейшем вручную.

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

Настройка Сервера администрирования

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

Настройка параметров подключения Kaspersky Security Center 14 Web Console к Серверу администрирования

Чтобы задать порты подключения к Серверу администрирования:

1. В верхней части экрана нажмите на значок настройки параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Порты подключения**.

Будут отображены основные параметры подключения к выбранному Серверу Администрирования.

Настройка списка разрешенных IP-адресов для подключения к Kaspersky Security Center

По умолчанию подключения к Kaspersky Security Center разрешены с любого устройства. Например, вы можете установить Сервер Kaspersky Security Center 14 Web Console на любое устройство, которое соответствует требованиям, и Сервер Kaspersky Security Center 14 Web Console будет взаимодействовать с Kaspersky Security Center. Также вы можете настроить Сервер администрирования так, чтобы подключения разрешались только с устройств с указанными вами IP-адресами. В этом случае, если злоумышленники попытаются подключиться к Kaspersky Security Center через Сервер Kaspersky Security Center 14 Web Console, установленный на устройстве, которое не включено в список разрешенных, они не смогут войти в Kaspersky Security Center.

IP-адрес проверяется, когда пользователь входит в Kaspersky Security Center или запускает программу, которая взаимодействует с Сервером администрирования через Kaspersky Security Center OpenAPI. В этот момент программа на устройстве пытается установить соединение с Сервером администрирования. Если IP-адрес устройства отсутствует в списке разрешенных, возникает ошибка аутентификации и событие KLAUD_EV_SERVERCONNECT уведомляет о том, что соединение с Сервером администрирования не установлено.

Требования к списку разрешенных IP-адресов

IP-адреса проверяются только при попытке подключения к Серверу администрирования следующих программ:

- Сервер Kaspersky Security Center 14 Web Console

  Если вы входите в Kaspersky Security Center через Kaspersky Security Center 14 Web Console, вы можете настроить сетевой экран на устройстве, где установлен Сервер Kaspersky Security Center 14 Web Console, штатными средствами операционной системы. Затем, если кто-то попытается войти в Kaspersky Security Center на одном устройстве, а Сервер Kaspersky Security Center 14 Web Console установлен на другом устройстве, сетевой экран поможет предотвратить вмешательство злоумышленников.

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

- Программы, взаимодействующие с Сервером администрирования через OpenAPI, такие как Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред.

Поэтому укажите адреса устройств, на которых установлены перечисленные выше программы.

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

Как создать список разрешенных IP-адресов

Если вы еще не установили список разрешенных, следуйте приведенным ниже инструкциям.

Чтобы создать список разрешенных IP-адресов для входа в Kaspersky Security Center:

1. На устройстве Сервера администрирования запустите командную строку под учетной записью с правами администратора.
2. Измените текущую папку на папку установки Kaspersky Security Center (обычно это /opt/kaspersky/ksc64/sbin).
3. Введите следующую команду 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.

Настройка журнала событий подключения к Серверу администрирования

Можно сохранить в файл журнала историю подключений и попыток подключения к Серверу администрирования в процессе его работы. Информация в файле позволит отследить не только подключения внутри инфраструктуры сети, но и попытки несанкционированного доступа к серверам.

Чтобы настроить регистрацию событий подключения к Серверу администрирования:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Порты подключения**.

3. Включите параметр **Записывать события соединения с Сервером администрирования в журнал**.

Все последующие события входящих подключений к Серверу администрирования, результаты аутентификации и ошибки SSL будут записываться в файл /var/opt/kaspersky/klnagent_srv/logs/sc.syslog.

Настройка количества событий в хранилище событий

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программа 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.

Программа проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, программа удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

Чтобы ограничить количество событий, которые можно сохранить в хранилище событий на Сервере администрирования:

1. В верхней части экрана нажмите на значок настройки параметров () рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Хранилище событий**. Укажите максимальное количество событий, хранящихся в базе данных.

3. Нажмите на кнопку **Сохранить**.

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 восстановить данные при переносе базы данных Сервера администрирования на другое устройство или при переходе на новую версию Kaspersky Security Center (перенос данных Сервера администрирования под управление Kaspersky Security Center Windows не поддерживается).

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.

Прежде чем создавать резервную копию данных Сервера администрирования, проверьте, добавлен ли виртуальный Сервер администрирования в группу администрирования. Если виртуальный Сервер администрирования добавляется перед резервным копированием, убедитесь, что этому виртуальному Серверу назначен администратор. Вы не можете предоставить права администратора к виртуальному Серверу администрирования после резервного копирования. Обратите внимание, если учетные данные администратора утеряны, вы не сможете назначить нового администратора виртуальному Серверу администратора.

Вы можете создать резервную копию данных Сервера администрирования одним из следующих способов:

- Создать и запустить задачу резервного копирования данных через Kaspersky Security Center 14 Web Console.
- Запустить утилиту klbackup на устройстве, где установлен Сервер администрирования. Утилита входит в состав комплекта поставки Kaspersky Security Center. После установки Сервера администрирования утилита находится в корне папки назначения, указанной при установке программы (обычно, /opt/kaspersky/ksc64/sbin/klbackup).

В резервной копии данных Сервера администрирования сохраняются следующие данные:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);

- конфигурационная информация о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки;
- сертификат Сервера администрирования.

Восстановление данных Сервера администрирования возможно только с помощью утилиты klbackup.

Создание задачи резервного копирования данных Сервера администрирования

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

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. Перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В списке **Программа** выберите **Kaspersky Security Center 14** 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 **Завершение создания задачи** на шаге **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 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. Дополнительные сведения см. в разделе Как восстановить данные Сервера администрирования из резервной копии, созданной на более ранней версии СУБД.

При использовании утилиты klbackup флаги Агента администрирования не восстанавливаются. Вам необходимо вручную настроить флаги Агента администрирования.

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 [-linux_path LINUX_PATH][-node_cert CERT_PATH] [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
```

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 или использовать для восстановления данные из папки BACKUP_PATH (обязательный параметр).
- `-linux_path LINUX_PATH` – локальный путь к папке с данными резервной копии данных СУБД.

  Учетная запись сервера базы данных и утилита klbackup должны обладать правами на изменение данных в папке LINUX_PATH.
- `-node_cert CERT_PATH` – файл сертификата Сервера для настройки неактивного узла отказоустойчивого кластера после восстановления. Если параметр не указан, он будет автоматически получен с Сервера.
- `-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` (в формате UTC). 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 `/tmp/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` – пароль для защиты конфиденциальных данных.

  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. Для восстановления данных Сервера администрирования из резервной копии рекомендуется запускать утилиту на только что установленном Сервере администрирования.

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 базы данных на новое устройство (сервер базы данных может быть установлен на новом устройстве вместе с Сервером администрирования или на другом устройстве).
- 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 с помощью Kaspersky Security Center 14 Web Console или запустите утилиту klbackup.
2. На предыдущем устройстве отключите Сервер администрирования от сети.
3. 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 14 Web Console и Агента администрирования. Проверьте, что порты, используемые на Сервере администрирования доступны.
4. Назначьте новому устройству тот же адрес.

   Новому Серверу администрирования можно присвоить имя NetBIOS, FQDN и статический IP-адрес. Это зависит от того, какой адрес Сервера администрирования был установлен в инсталляционном пакете Агента администрирования, когда были развернуты Агенты администрирования. Также вы можете использовать адрес подключения, определяющий Сервер администрирования, к которому подключается Агент администрирования (вы можете получить этот адрес на управляемых устройствах с помощью утилиты klnagchk).

5. При необходимости на другом устройстве установите систему управления базами данных (СУБД), которую будет использовать Сервер администрирования.

   База данных может быть установлена на новом устройстве вместе с Сервером администрирования или на другом устройстве. Убедитесь, что это устройство соответствует аппаратным и программным требованиям. При выборе СУБД учитывайте количество устройств, которые обслуживает Сервер администрирования.

6. Установите Сервер администрирования на новое устройство.

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

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

8. Откройте Kaspersky Security Center 14 Web Console и подключитесь к Серверу администрирования.

9. Убедитесь, что все управляемые устройства подключены к Серверу администрирования.

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

Создание виртуального Сервера администрирования

Можно создать виртуальные Серверы администрирования и добавить их в группы администрирования.

Чтобы создать и добавить виртуальный Сервер администрирования:

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

2. На открывшейся странице перейдите на закладку **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.

   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.

6. 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 14 Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- Измените существующую установку Kaspersky Security Center 14 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center 14 Web Console.

  1. На устройстве, где установлена программа Kaspersky Security Center 14 Web Console, запустите установочный файл Web Console, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки программы. Для продолжения работы мастера нажмите на кнопку **Далее**.

  2. Выберите параметр **Обновить**.

  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.

  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.

  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.

  6. После успешного завершения настройки программы нажмите кнопку **Готово**.

- Используйте Kaspersky Security Center 14 Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center 14 Web Console.

Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию.

В иерархии Сервер администрирования Kaspersky Security Center Linux может работать только как подчиненный Сервер под управлением главного Сервера администрирования Kaspersky Security Center на базе Windows или Kaspersky Security Center Cloud Console.

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

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Главный Сервер администрирования получает данные только от не виртуальных 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

Развернуть все | Свернуть все

В иерархии Сервер администрирования Kaspersky Security Center Linux может работать только как подчиненный Сервер под управлением главного Сервера администрирования Kaspersky Security Center на базе Windows или Kaspersky Security Center Cloud Console.

Добавление подчиненного Сервера администрирования (выполняется с будущим главным Сервером администрирования)

Вы можете добавить Сервер администрирования в качестве подчиненного Сервера, установив таким образом отношение иерархии "главный Сервер – подчиненный Сервер".

Чтобы добавить Сервер администрирования, доступный для подключения через Kaspersky Security Center 14 Web Console, в качестве подчиненного Сервера:

1. Убедитесь, что порт 13000 будущего главного Сервера доступен для приема подключений от подчиненных Серверов администрирования.
2. На будущем главном Сервере администрирования нажмите на значок параметров ( ).
3. На открывшейся странице свойств нажмите на закладку **Серверы администрирования**.
4. Установите флажок рядом с именем группы администрирования, в которую вы хотите добавить Сервер администрирования.
5. В меню выберите пункт **Подключить подчиненный Сервер администрирования**.

   Запустится мастер добавления подчиненного Сервера администрирования. Для продолжения работы мастера нажмите на кнопку **Далее**.
6. Заполните следующие поля:
   - **Имя подчиненного Сервера администрирования**

     Имя подчиненного Сервера администрирования, которое будет отображаться в иерархии Серверов. Вы можете ввести IP-адрес в качестве имени или использовать такое имя, как, например, "Подчиненный Сервер для группы 1".
   - **Адрес подчиненного Сервера администрирования (необязательно)**

     Укажите IP-адрес или доменное имя подчиненного Сервера администрирования.

     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**
  - **Имя пользователя**
  - **Пароль**

7. Следуйте далее указаниям мастера.

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 или недоступен), вы все равно можете добавить подчиненный Сервер администрирования.

Чтобы добавить Сервер администрирования, недоступный для подключения через Kaspersky Security Center 14 Web Console, в качестве подчиненного Сервера:

1. Отправьте файл сертификата будущего главного Сервера администрирования системному администратору офиса, в котором находится будущий подчиненный Сервер администрирования. (Например, вы можете записать файл на внешнее устройство или отправить его по электронной почте.)

   Файл сертификата находится на будущем главном Сервере администрирования, /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Предложите системному администратору, ответственному за будущий подчиненный Сервер администрирования, следующее:

   a. Нажмите на значок параметров ( ).

   b. На открывшейся странице свойств перейти в раздел **Иерархия Серверов администрирования** на закладке **Общие**.

   c. Выберите параметр **Данный Сервер администрирования является подчиненным в иерархии**.

   d. В поле **Адрес главного Сервера администрирования** введите сетевое имя будущего главного Сервера администрирования.

   e. Выбрать ранее сохраненный файл сертификата будущего главного Сервера, нажав на кнопку **Обзор**.

   f. Если необходимо, установить флажок **Подключать главный Сервер к подчиненному Серверу в демилитаризованной зоне**.

   g. Если подключение к будущему подчиненному Серверу администрирования выполняется с помощью прокси-сервера, выберите параметр **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.

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 14 Web Console и не можете подключиться к виртуальному Серверу администрирования, управляемому подчиненным Сервером администрирования, вы можете воспользоваться одним из следующих способов:

- **Измените существующую установку Kaspersky Security Center 14 Web Console, добавив подчиненный Сервер в список доверенных Серверов администрирования**. После этого вы сможете подключиться к виртуальному Серверу администрирования в Kaspersky Security Center 14 Web Console.

  1. На устройстве, где установлена программа Kaspersky Security Center 14 Web Console, запустите установочный файл Web Console, соответствующий дистрибутиву Linux, установленному на вашем устройстве, под учетной записью с правами администратора.

     Запустится мастер установки программы. Для продолжения работы мастера нажмите на кнопку **Далее**.
  2. Выберите параметр **Обновить**.
  3. На странице **Тип изменения** выберите параметр **Изменить параметры подключения**.
  4. На шаге **Доверенные Серверы администрирования** добавьте требуемый подчиненный Сервер администрирования.
  5. На последнем шаге нажмите на кнопку **Изменить**, чтобы применить новые параметры.
  6. После успешного завершения настройки программы нажмите кнопку **Готово**.

- Используйте Kaspersky Security Center 14 Web Console, чтобы напрямую подключиться к подчиненному Серверу администрирования, на котором был создан виртуальный Сервер. После этого вы сможете переключиться на виртуальный Сервер администрирования в Kaspersky Security Center 14 Web Console.

Включение защиты учетной записи от несанкционированного изменения

Вы можете дополнительно включить защиту учетной записи пользователя от несанкционированного изменения. Если этот параметр включен, изменение параметров учетной записи пользователя требует авторизации пользователя с правами на изменение.

Чтобы включить или выключить защиту учетной записи от несанкционированного изменения:

1. В главном окне программы перейдите в раздел **Пользователи и роли → Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите настроить защиту учетной записи от несанкционированного изменения.
3. В открывшемся окне свойств пользователя выберите закладку **Проверка подлинности**.
4. На закладке **Проверка подлинности** 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 14 Web Console.

О двухэтапной проверке учетной записи

Kaspersky Security Center Linux предоставляет двухэтапную проверку для пользователей Kaspersky Security Center 14 Web Console. Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center 14 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 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 программу, Сервер администрирования сохраняет новый секретный ключ для учетной записи пользователя. Если пользователь неправильно ввел новый секретный ключ, Сервер администрирования не сохраняет новый секретный ключ и оставляет текущий секретный ключ действующим для дальнейшей аутентификации.

Любое программное обеспечение для аутентификации, которое поддерживает алгоритм одноразового пароля на основе времени (TOTP), может использоваться в качестве приложения 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 для аутентификации.

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.

Настоятельно рекомендуется сохранить секретный ключ или QR-код и хранить его в надежном месте. Это поможет вам восстановить доступ к Kaspersky Security Center 14 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 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 14 Web Console с помощью двухэтапной проверки, может выключать двухэтапную проверку: для любого другого пользователя, только если двухэтапная проверка для всех пользователей выключена; для пользователя, исключенного из списка двухэтапной проверки включенной для всех пользователей.
- Любой пользователь, выполнивший вход в Kaspersky Security Center 14 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.

Сценарий: Настройка двухэтапной проверки для всех пользователей

В этом сценарии описывается, как включить двухэтапную проверку для всех пользователей и как исключить учетные записи пользователей из двухэтапной проверки. Если вы не включили двухэтапную проверку для своей учетной записи, прежде чем включить ее для других пользователей, программа сначала откроет окно включения двухэтапной проверки для вашей учетной записи. В этом сценарии также описано, как включить двухэтапную проверку для вашей учетной записи.

Если вы включили двухэтапную проверку для своей учетной записи, вы можете перейти к включению двухэтапной проверки для всех пользователей.

Предварительные требования

Прежде чем начать:

- Убедитесь, что ваша учетная запись имеет право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей** для изменения параметров безопасности учетных записей других пользователей.
- Убедитесь, что другие пользователи Сервера администрирования установили на свои устройства приложение 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 для аутентификации, 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 для аутентификации.

   Категорически не рекомендуется устанавливать приложение для аутентификации на том же устройстве, с которого выполняется подключение к Серверу администрирования.

2. **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.

3. **Включение двухэтапной проверки и получение секретного ключа для своей учетной записи**

   После включения двухэтапной проверки для своей учетной записи вы можете включить двухэтапную проверку для всех пользователей.

4. **Включение двухэтапной проверки для всех пользователей**

   Пользователи с включенной двухэтапной проверкой должны использовать ее для входа на Сервер администрирования.

5. **Изменение имени издателя кода безопасности**

Если у вас несколько Серверов администрирования с похожими именами, возможно, вам придется изменить имена издателей кода безопасности для лучшего распознавания разных Серверов администрирования.

6. **Исключение учетных записей пользователей, для которых не требуется включать двухэтапную проверку**

   При необходимости исключите учетные записи пользователей из двухэтапной проверки. Пользователям с исключенными учетными записями не нужно использовать двухэтапную проверку для входа на Сервер администрирования.

7. **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 14 Web Console. 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.

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 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 программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на имя вашей учетной записи.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Проверка подлинности**:
   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 для аутентификации или нажмите **Просмотреть QR-код** и отсканируйте QR-код с помощью приложения для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   c. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации и нажмите на кнопку **Проверить и применить**.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи включена.

Включение обязательной двухэтапной проверки для всех пользователей

Вы можете включить двухэтапную проверку для всех пользователей Сервера администрирования, если у вашей учетной записи есть право Изменение списков управления доступом объектов в функциональной области **Общий функционал: Права пользователей** и если вы выполнили аутентификацию с помощью двухэтапной проверки.

Чтобы включить двухэтапную проверку для всех пользователей:

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

   Откроется окно свойств Сервера администрирования.
2. На закладке **Проверка подлинности** окна свойств включите **двухэтапную проверку для всех пользователей**.

3. Если вы не включили двухэтапную проверку для своей учетной записи, программа откроет окно включения двухэтапной проверки для вашей учетной записи.

   a. В открывшемся окне двухэтапной проверки нажмите **Узнайте, как настроить двухэтапную проверку**.

   b. Нажмите на кнопку **Просмотреть QR-код**.

   c. Отсканируйте QR-код приложением для аутентификации на мобильном устройстве, чтобы получить одноразовый код безопасности.

   Введите секретный ключ в приложение для аутентификации вручную.

   d. В окне двухэтапной проверки укажите код безопасности, сгенерированный приложением для аутентификации 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 из двухэтапной проверки.

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 другой учетной записи пользователя, 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 выключить двухэтапную проверку для учетной записи пользователя:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись внутреннего пользователя, для которой вы хотите выключить двухэтапную проверку. Это может быть ваша собственная учетная запись или учетная запись любого другого пользователя.
3. В открывшемся окне свойств пользователя выберите закладку **Защита учетной записи**.
4. На закладке **Защита учетной записи** выберите параметр **Запрашивать только имя пользователя и пароль**, если вы хотите выключить двухэтапную проверку для учетной записи пользователя.
5. Нажмите на кнопку **Сохранить**.

Двухэтапная проверка для вашей учетной записи выключена.

Если вы хотите восстановить доступ пользователя, который не может войти в Kaspersky Security Center 14 Web Console с помощью двухэтапной проверки, выключите двухэтапную проверку для этой учетной записи пользователя и выберите параметр **Запрашивать только имя пользователя и пароль** как описано выше. После этого войдите в Kaspersky Security Center 14 Web Console под учетной записью пользователя, для которого вы выключили двухэтапную проверку и снова включите проверку.

Выключение обязательной двухэтапной проверки для всех пользователей

Вы можете выключить обязательную 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 записи, прежде чем выключить ее для всех пользователей.

Чтобы выключить двухэтапную проверку для всех пользователей:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Проверка подлинности** 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. Выключение двухэтапной проверки для всех пользователей не применяется к конкретным учетным записям, для которых двухэтапная проверка ранее была включена отдельно.

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 **Проверка подлинности** 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.

Генерация нового секретного ключа

Вы можете сгенерировать новый секретный ключ для двухэтапной проверки своей учетной записи, только если вы авторизованы с помощью двухэтапной проверки.

Чтобы сгенерировать новый секретный ключ для учетной записи пользователя:

1. В главном окне программы перейдите в раздел **Пользователи и роли → Пользователи**.

2. Нажмите на учетную запись пользователя, для которой вы хотите сгенерировать новый секретный ключ для двухэтапной проверки.

3. В открывшемся окне свойств пользователя выберите закладку **Проверка подлинности**.

4. На вкладке **Проверка подлинности** перейдите по ссылке **Сгенерировать 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 мобильное устройство, можно установить приложение для аутентификации на другое мобильное устройство и сгенерировать новый секретный ключ для восстановления доступа к Kaspersky Security Center 14 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 закладку **Защита учетной записи**.

3. На вкладке **Защита учетной записи** перейдите по ссылке **Изменить**.

   Откроется раздел **Изменить издателя кода безопасности**.

4. Укажите новое имя издателя кода безопасности.

5. Нажмите на кнопку **OK**.

Для Сервера администрирования указано новое имя издателя кода безопасности.

Изменение количества попыток ввода пароля

Пользователь Kaspersky Security Center Linux 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.

Изменение учетных данных СУБД

Иногда может потребоваться изменить учетные данные СУБД, например, чтобы выполнить ротацию учетных данных в целях безопасности.

Чтобы изменить учетные данные СУБД в среде Linux с помощью утилиты klsrvconfig:

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

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

Учетные данные СУБД изменены.

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 верхней части экрана нажмите на значок параметров () рядом с именем главного Сервера администрирования.
2. На открывшейся странице перейдите на закладку **Серверы администрирования**.
3. В группе администрирования, в которой вы хотите удалить подчиненный Сервер администрирования, выберите подчиненный Сервер администрирования.
4. В меню выберите пункт **Удалить**.
5. В открывшемся окне нажмите на кнопку **OK** для подтверждения удаления подчиненного Сервера администрирования.

Бывший главный Сервер администрирования и бывший подчиненный Сервер администрирования теперь независимы друг от друга. Иерархии Серверов больше не существует.

Настройка интерфейса

Вы можете настроить интерфейс Kaspersky Security Center 14 Web Console на отображение и скрытие разделов и элементов интерфейса в зависимости от используемых функций.

Чтобы настроить интерфейс Kaspersky Security Center 14 Web Console в соответствии в соответствии с используемым в настоящее время набором функций:

1. В главном меню нажмите на меню учетной записи.

2. В раскрывающемся меню выберите пункт **Параметры интерфейса**.

3. В появившемся окне **Параметры интерфейса** включите или выключите необходимые параметры.

4. Нажмите на кнопку **Сохранить**.

После этого в консоли отображаются разделы в главном меню в соответствии с включенными параметрами. Например, если включить **Показать EDR-обнаружения**, раздел **Мониторинг и отчеты** → **Обнаружения** появится в главном меню.

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.

Сценарий: Обнаружение сетевых устройств

Вы должны выполнить поиск устройств перед установкой программ безопасности. При обнаружении сетевых устройств можно получить о них информацию и управлять ими с помощью политик. Регулярные опросы сети необходимы для проверки появления новых устройств и наличия обнаруженных ранее устройств в сети.

Обнаружение сетевых устройств состоит из следующих этапов:

1. **Первоначальное обнаружение устройств**

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

2. **Настройка будущих опросов**

   Убедитесь, что опрос IP-диапазонов 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, если в вашей сети есть IPv6-устройства.

3. **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 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 Linux обнаруживает устройства в сети и предоставляет информацию о них.
- Настроены будущие опросы сети и расписание их запуска.

Новые обнаруженные устройства распределены в соответствии с заданными правилами. Если правила не заданы, устройства остаются в группе **Нераспределенные устройства**.

Опрос IP-диапазонов

Развернуть все | Свернуть все

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 устройств.

Просмотр и изменение параметров опроса IP-диапазонов

Чтобы просмотреть и изменить параметры опроса IP-диапазонов:

1. 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. Если IP-адрес не подтвержден при опросе в течение времени действия IP-адреса, он автоматически удаляется из результатов опроса. По умолчанию срок существования запросов составляет 24 часа, поскольку динамические IP-адреса, назначенные по протоколу DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации сетевого узла), меняются каждые 24 часа.

   Варианты расписания опроса:

   - **Каждые N дней**

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

     По умолчанию опрос запускается каждые шесть часов, начиная с текущей системной даты и времени.
   - **Каждые N минут**

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

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

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

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

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

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

     По умолчанию параметр выключен.
5. Нажмите на кнопку **Сохранить**.

Параметры будут сохранены и применены ко всем IP-диапазонам.

Запуск опроса вручную

Чтобы запустить проверку немедленно,

нажмите на кнопку **Начать опрос**.

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, Kaspersky Security Center будет опрашивать всю сеть.

Чтобы добавить новый IP-диапазон:

1. 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. 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.
4. 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.
5. Нажмите на кнопку **Сохранить**.

IP-диапазон добавлен в список IP-диапазонов.

Вы можете запустить опрос для каждого IP-диапазона в отдельности, используя кнопку **Начать опрос**. После завершения опроса вы можете просмотреть список обнаруженных устройств, нажав на кнопку **Устройства**. По умолчанию срок действия результатов опроса составляет 24 часа, он равен времени действия IP-адреса.

Чтобы добавить подсеть в существующий IP-диапазон:

1. 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 (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. 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.

Теги устройств

В этом разделе описаны теги устройств, приведены инструкции по их созданию и изменению, а также по назначению тегов устройствам вручную и автоматически.

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, при поиске устройств и при распределении устройств по группам администрирования.

Теги могут назначаться устройствам вручную или автоматически. Теги можно назначать вручную, если требуется отметить отдельные устройства. Автоматическое назначение тегов выполняется Kaspersky Security Center в соответствии с заданными правилами назначения тегов.

Автоматическое назначение тегов устройствам происходит при выполнении определенных правил. Каждому тегу соответствует отдельное правило. Правила могут применяться к сетевым свойствам устройства, операционной системе, установленным на устройстве программам и другим свойствам устройства. Например, вы можете настроить правило, в соответствии с которым устройствам, работающим под управлением операционной системы CentOS, назначается тег `[CentOS]`. Затем можно использовать этот тег при создании выборки устройств, чтобы отобрать все устройства под управлением операционной системы CentOS и назначить им задачу.

Тег автоматически удаляется с устройства в следующих случаях:

- Устройство перестает удовлетворять условиям правила назначения тега.
- Правило назначения тега выключено или удалено.

Списки тегов и списки правил для каждого Сервера администрирования являются независимыми для всех Серверов администрирования, включая главный Сервер администрирования и подчиненные виртуальные Серверы администрирования. Правило применяется только к устройствам под управлением того Сервера администрирования, на котором оно создано.

Создание тегов устройств

Чтобы создать тег устройства:

1. В главном окне программы перейдите в раздел **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.

Изменение тегов устройств

Чтобы переименовать тег устройства:

1. В главном окне программы перейдите в раздел **Устройства → Теги → Теги устройств**.

2. Выделите тег, который требуется переименовать.

   Откроется окно свойств тега.

3. В поле **Тег** измените название тега.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов устройства.

Удаление тегов устройств

Чтобы удалить тег устройства:

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.

2. В списке выберите теги устройства, которые вы хотите удалить.

3. Нажмите на кнопку **Удалить**.

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

Выбранный тег устройства удален. Удаленный тег автоматически снимается со всех устройств, которым он был назначен.

> Тег, который вы удалили, не удаляется автоматически из правил автоматического назначения тегов. После удаления тега он будет назначен новому устройству только при первом совпадении параметров устройства с условиями правила назначения тегов.

> Удаленный тег не удаляется автоматически с устройства, если этот тег назначен устройству программой или Агентом администрирования. Для того чтобы удалить тег с вашего устройства, используйте утилиту klscflag.

Просмотр устройств, которым назначен тег

Чтобы просмотреть устройства с назначенными тегами:

1. В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Теги устройств**.

2. Перейдите по ссылке **Просмотреть 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.

Просмотр тегов, назначенных устройству

Чтобы просмотреть теги, назначенные устройству:

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

2. Выберите устройство, теги которого требуется просмотреть.

3. В открывшемся окне свойств устройства выберите закладку **Теги**.

Отобразится список тегов, назначенных выбранному устройству. В столбце **Назначенный тег** вы можете просмотреть, как был назначен тег.

Можно назначить другой тег устройству или удалить назначенный ранее тег. Можно также просмотреть все теги устройств, которые существуют на Сервере администрирования.

Вы также можете просмотреть теги, назначенные устройству, в командной строке с помощью утилиты klscflag.

Чтобы просмотреть в командной строке теги, назначенные устройству, выполните следующую команду:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvget -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt
ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

Назначение тегов устройству вручную

Чтобы вручную назначить тег устройству:

1. Просмотрите теги, уже назначенные устройству, которому вы ходите назначить тег.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне выполните одно из следующих действий:
   - Чтобы создать и назначить новый тег, выберите пункт **Создать тег** и укажите тег.
   - 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.

Удаление назначенного тега с устройства

Чтобы снять назначенный тег с устройства:

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите устройство, теги которого требуется просмотреть.
3. В открывшемся окне свойств устройства выберите закладку **Теги**.
4. Установите флажок напротив тега, который требуется снять.
5. В верхней части списка нажмите на кнопку **Отменить назначение тега**.
6. В появившемся окне нажмите на кнопку **Да**.

Тег будет снят с устройства.

Снятый с устройства тег не удаляется. При необходимости его можно удалить вручную.

Вы не можете вручную удалить теги, назначенные устройству программами или Агентом администрирования. Для того чтобы удалить эти теги, используйте утилиту klscflag.

Просмотр правил автоматического назначения тегов устройствам

Чтобы просмотреть правила автоматического назначения тегов устройствам,

Выполните одно из следующих действий:

- В главном окне программы перейдите в раздел **Устройства** → **Теги** → **Правила автоматического назначения тегов**.
- В главном окне программы перейдите в раздел **Устройства** → **Теги** и перейдите по ссылке **Настроить правила автоматического назначения тегов**.
- Перейдите к просмотру тегов, назначенных устройству, и нажмите на кнопку **Параметры**.

Отобразится список правил автоматического назначения тегов устройствам.

Изменение правил автоматического назначения тегов устройствам

Чтобы изменить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
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.
- Если вы хотите изменить существующее условие, выделите условие, которое требуется изменить, и измените его параметры.
- 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 **OK**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененное правило отображается в списке.

Создание правил автоматического назначения тегов устройствам

Чтобы создать правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.

2. Нажмите на кнопку **Добавить**.

Откроется окно с параметрами нового правила.

3. Укажите основные параметры правила:

a. В поле **Имя правила** введите название правила.

Название не должно быть длиннее 256 символов.

b. Выполните одно из следующих действий:

- Включите правило, установив переключатель в положение **Правило включено**.
- Выключите правило, установив переключатель в положение **Правило выключено**.

c. В поле **Тег** укажите новое название тега устройства или выберите существующий тег устройства из списка.

Название не должно быть длиннее 256 символов.

4. В поле выбора условия нажмите на кнопку **Добавить**, чтобы добавить новое условие.

Откроется окно с параметрами нового условия.

5. Укажите название условия.

Название не должно быть длиннее 256 символов. Название условия должно быть уникальным в рамках одного правила.

6. Настройте срабатывание правила по следующим условиям. Можно выбрать несколько условий.

- **Сеть** – сетевые свойства устройства (например, DNS-имя устройства или принадлежность устройства к IP-подсети).

> Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правила автоматического назначения тегов не будет работать.

- **Программы** – наличие на устройстве Агента администрирования, тип, версия и архитектура операционной системы.
- **Виртуальные машины** – принадлежность устройства к определенному типу виртуальных машин.
- **Реестр программ** – наличие на устройстве программ различных производителей.

7. Нажмите на кнопку **OK**, 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.
- После выполнения правила вручную.
- 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 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.
2. Установите флажки напротив активных правил, которые требуется выполнить.
3. Нажмите на кнопку **Выполнить правило**.

Выбранные правила будут выполнены.

Удаление правил автоматического назначения тегов с устройств

Чтобы удалить правило автоматического назначения тегов устройствам:

1. Просмотрите правила автоматического назначения тегов устройствам.
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.

Управление тегами устройств с помощью утилиты klscflag

Чтобы назначить набор тегов устройству, вам нужно запустить утилиту klscflag на клиентском устройстве, которому вы хотите назначить теги.

Утилита klscflag перезаписывает существующие теги, назначенные устройству. Это означает, что вы можете добавить или удалить теги, указав нужный набор тегов в команде. Утилита не имеет команд для добавления или удаления отдельных тегов. Вы изменяете весь набор тегов.

> При указании тегов в командах, таких как klscflag, рекомендуется использовать символы одного регистра, например все буквы заглавные. Использование всех заглавных букв поможет избежать возможных проблем с тегами, которые отличаются только регистром, в зависимости от конфигурации СУБД.

Чтобы назначить один или несколько тегов вашему устройству с помощью утилиты klscflag:

1. Запустите командную строку под учетной записью с правами root и измените текущую директорию на директорию с утилитой klscflag. Утилита klscflag расположена в директории установки Агента администрирования. По умолчанию директория установки – /opt/kaspersky/ksc64/sbin.

2. Введите одну из следующих команд:

- Чтобы назначить набор тегов:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ТЕГ 1\",\"ТЕГ 2\",\"ТЕГ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

  где `[\"ТЕГ 1\",\"ТЕГ 2\",\"ТЕГ 3\"]` это список тегов, которые вы хотите назначить устройству.

  Если вы оставите квадратные скобки пустыми, это удалит все теги с устройства:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

- Чтобы назначить новый тег существующему набору тегов:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"НОВЫЙ ТЕГ\",\"ТЕГ 1\",\"ТЕГ 2\",\"ТЕГ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

  где `НОВЫЙ ТЕГ` – это тег, который вы хотите назначить устройству, `ТЕГ 1`, `ТЕГ 2`, `ТЕГ 3` – это теги, которые уже назначены устройству.

- Чтобы удалить определенный тег, не удаляя другие теги, уже назначенные устройству, выполните команду с обновленным набором тегов.

  Например, если `ТЕГ 1`, `ТЕГ 2`, `ТЕГ 3` – ваши текущие теги и вы хотите удалить `ТЕГ 2`, выполните следующую команду:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"ТЕГ 1\",\"ТЕГ 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Перезапустите службу Агента администрирования.

Утилита klscflag назначит вашему устройству указанные теги. Чтобы убедиться, что утилита klscflag успешно назначила указанные теги, просмотрите теги, которые были назначены устройству.

Также можно назначать теги устройств вручную.

Теги программ

В этом разделе описаны теги программ, приведены инструкции по их созданию и изменению, а также по назначению тегов сторонним программам.

Теги программ

Kaspersky Security Center Linux позволяет назначать теги программам из реестра программ. Тег представляет собой метку программы, которую можно использовать для группировки и поиска программ. Назначенный программе тег можно использовать в условиях для выборок устройств.

Например, можно создать тег `[Браузеры]` и назначить его всем браузерам, таким как Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Создание тегов программ

Чтобы создать тег программы:

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Теги программ**.
2. Нажмите на кнопку **Добавить**.

   Отобразится окно создания тега.
3. Укажите тег.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Новый созданный тег появляется в списке тегов программы.

Изменение тегов программ

Чтобы переименовать тег программы:

1. В главном окне программы перейдите в раздел **Операции** → **Программы сторонних производителей** → **Теги программ**.
2. Установите флажок рядом с тегом, который вы хотите переименовать, и нажмите на кнопку **Изменить**.

   Откроется окно свойств тега.
3. Измените имя тега.
4. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Обновленный тег появится в списке тегов программ.

Назначение тегов программам

Чтобы назначить программе теги:

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Реестр программ**.
2. Выберите программу, для которой требуется назначить теги.
3. Выберите закладку **Теги**.

   На закладке появятся все теги программ, существующие на Сервере администрирования. Теги, назначенные выбранной программе, отмечены флажками в графе **Назначенный тег**.
4. Установите флажки в графе **Назначенный тег** для тегов, которые требуется назначить.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги назначены программе.

Снятие назначенных тегов с программ

Чтобы снять теги с программы:

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Реестр программ**.
2. Выберите программу, с которой требуется снять теги.
3. Выберите закладку **Теги**.

   На закладке появятся все теги программ, существующие на Сервере администрирования. Теги, назначенные выбранной программе, отмечены флажками в графе **Назначенный тег**.
4. Снимите флажки в графе **Назначенный тег** для тегов, которые требуется снять.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Теги будут сняты с программы.

> Снятые с программ теги не удаляются. При необходимости их можно удалить вручную.

Удаление тегов программ

Чтобы удалить тег программы:

1. В главном окне программы перейдите в раздел **Операции → Программы сторонних производителей → Теги программ**.
2. В списке выберите теги программы, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Выбранный тег программы удален. Удаленный тег автоматически снимается со всех программ, которым он был назначен.

Развертывание программ "Лаборатории Касперского"

В этом разделе описано, как развернуть программы "Лаборатории Касперского" на клиентских устройствах в вашей организации с помощью Kaspersky Security Center 14 Web Console.

Сценарий: Развертывание программ "Лаборатории Касперского"

В этом сценарии описана процедура развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14 Web Console. Можно либо воспользоваться мастером первоначальной настройки и мастером развертывания защиты, либо выполнить все необходимые шаги вручную.

Развертывание программ "Лаборатории Касперского" состоит из следующих этапов:

1. **Загрузка веб-плагина управления программы**

Загрузите веб-плагин управления Kaspersky Endpoint Security для Linux с сайта "Лаборатории Касперского" и добавьте плагин в Kaspersky Security Center 13 Web Console.

2. **Загрузка и создание инсталляционных пакетов для Агента администрирования**

   Загрузите дистрибутив Агента администрирования с сайта "Лаборатории Касперского" и создайте инсталляционный пакет Агента администрирования.

   Вы можете использовать загруженный инсталляционный пакет для локальной установки Агента администрирования. Для этого следуйте инструкциям, приведенным в документации Kaspersky Endpoint Security для Linux.

3. **Загрузка и создание инсталляционного пакета для Kaspersky Endpoint Security для Linux**

   Загрузите дистрибутив Kaspersky Endpoint Security для Linux с сайта "Лаборатории Касперского" и создайте инсталляционный пакет Kaspersky Endpoint Security для Linux.

4. **Создание автономного инсталляционного пакета (если требуется)**

   Если вы не можете установить программы "Лаборатории Касперского" с помощью Kaspersky Security Center Linux на некоторых устройствах, например, на устройствах удаленных сотрудников, вы можете создавать автономные установочные пакеты для программ. Если вы используете автономные пакеты для установки программ "Лаборатории Касперского" пропустите пункты 5 и 6 этого сценария.

5. **Создание, настройка и запуск задачи удаленной установки**

   Этот шаг входит в мастер развертывания защиты. Если вы не запускали мастер развертывания защиты, вам необходимо создать и настроить эту задачу вручную.

   Вы можете вручную создать несколько задач удаленной установки для различных групп администрирования или выборок устройств. Вы можете развернуть различные версии одной программы в этих задачах.

   Убедитесь, что все устройства в сети обнаружены, а затем запустите задачу (или задачи) удаленной установки.

   > Если вы хотите установить Агент администрирования на устройства с операционной системой SUSE Linux Enterprise Server 15, сначала установите пакет insserv-compat, чтобы настроить Агент администрирования.

6. **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 и настроить эту задачу вручную. Если вы запускали мастер первоначальной настройки, убедитесь, что расписание запуска задачи соответствует вашим требованиям. (По умолчанию для времени запуска задачи установлено значение **Вручную**, но вам может понадобиться изменить это значение.)

7. **Создание политик**

   Создайте политику Kaspersky Endpoint Security для Linux вручную или с помощью мастера первоначальной настройки. Можно использовать установленные по умолчанию параметры политики. Также вы можете в любое время изменить заданные по умолчанию параметры политики в соответствии с вашими требованиями.

8. **Проверка результатов**

   Убедитесь, что развертывание завершилось успешно: созданы политики и задачи для каждой программы и эти программы установлены на управляемые устройства.

Результаты

Завершение сценария дает следующее:

- Все требуемые политики и задачи для выбранных программ созданы.
- Расписание запуска задач настроено в соответствии с вашими требованиями.
- На выбранных клиентских устройствах развернуты или запланированы к развертыванию выбранные программы.

Добавление плагина управления для программ "Лаборатории Касперского"

Чтобы развернуть программу "Лаборатории Касперского", такую как Kaspersky Endpoint Security для Linux, необходимо загрузить веб-плагин управления для этой программы.

Чтобы добавить и установить веб-плагин управления для программы "Лаборатории Касперского":

1. Загрузите веб-плагин управления Kaspersky Endpoint Security для Linux с сайта "Лаборатории Касперского".
2. Откройте Kaspersky Security Center 14 Web Console.

3. В раскрывающемся списке **Параметры консоли** выберите **Веб-плагины**.

   Отобразится список доступных плагинов управления.

4. Нажмите на кнопку **Добавить из файла**.

   Отобразится окно **Добавить из файла**.

5. Нажмите на кнопку **загрузить файл формата ZIP**.

6. Укажите загруженный файл формата ZIP веб-плагина.

7. Нажмите на кнопку **Загрузить подпись**.

8. Укажите загруженный файл формата TXT подписи веб-плагина.

9. Нажмите на кнопку **Добавить**.

   Kaspersky Security Center проверяет загруженные файлы, а затем добавляет и устанавливает веб-плагин.

10. После завершения установки нажмите на кнопку **OK**.

Веб-плагин управления будет установлен в конфигурации по умолчанию и появится в списке веб-плагинов управления.

Создание инсталляционных пакетов из файла

Вы можете использовать пользовательские инсталляционные пакеты, чтобы:

- установить любую программу (такую как текстовый редактор) на клиентские устройства, например, с помощью задачи;
- создать автономный инсталляционный пакет .

Пользовательский инсталляционный пакет – это папка с набором файлов. Источником для создания пользовательского инсталляционного пакета является *архивный файл*. Архивный файл содержит файл или файлы, которые должны быть включены в пользовательский инсталляционный пакет.

Во время создания пользовательского инсталляционного пакета, вы можете указать параметры командной строки, например, для установки программы в тихом режиме.

Чтобы создать пользовательский инсталляционный пакет:

1. Выполните одно из следующих действий:

   - Перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - 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) нельзя.

   Начнется загрузка файла на Сервер администрирования.

6. Если вы указали файл программы "Лаборатории Касперского", вам может быть предложено прочитать и принять Лицензионное соглашение для этой программы. Чтобы продолжить, вы должны принять условия Лицензионного соглашения. Выберите параметр **Принять положения и условия настоящего Лицензионного соглашения**, только если вы полностью прочитали, понимаете и принимаете условия Лицензионного соглашения.

   Также вам будет предложено прочитать и принять условия Политики конфиденциальности. Чтобы продолжить, вы должны принять условия Политики конфиденциальности. Выберите параметр **Я принимаю Политику 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 программы из инсталляционного пакета в тихом режиме. Указывать параметры командной строки необязательно.

   Начнется процесс создания инсталляционного пакета.

В окне мастера отобразится информация о завершении процесса.

Если инсталляционный пакет не создан, отобразится соответствующее сообщение.

8. Нажмите на кнопку **Готово**, чтобы закрыть окно мастера.

Созданный инсталляционный пакет загружается во вложенную папку Packages общей папки Сервера администрирования. После загрузки инсталляционный пакет появится в списке инсталляционных пакетов.

В списке инсталляционных пакетов доступных на Сервере администрирования, нажав на имя инсталляционного пакета, вы можете:

- Просмотреть следующие свойства инсталляционного пакета:
  - **Имя**. Название инсталляционного пакета.
  - **Источник**. Имя поставщика программы.
  - **Программа**. Название программы, упакованной в пользовательский инсталляционные пакет.
  - **Версия**. Версия программы.
  - **Язык**. Язык программы, упакованной в пользовательский инсталляционный пакет.
  - **Размер (МБ)**. Размер инсталляционного пакета.
  - **Операционная система**. Тип операционной системы, для которой предназначен инсталляционные пакет.
  - **Создано**. Дата создания инсталляционного пакета.
  - **Изменено**. Дата изменения инсталляционного пакета.
  - **Тип**. Тип инсталляционного пакета.
- Измените параметры командной строки.

Создание автономного инсталляционного пакета

Вы и пользователи устройств в вашей организации можете использовать автономные инсталляционные пакеты для ручной установки программ на устройства.

Автономный инсталляционный пакет представляет собой исполняемый файл, который можно разместить на Веб-сервере или в общей папке, отправить по почте или передать на клиентское устройство другим способом. Полученный файл можно запустить локально на клиентском устройстве для выполнения установки программы без участия Kaspersky Security Center Linux. Вы можете создать автономный инсталляционный пакет для программ "Лаборатории Касперского", так и для программ сторонних производителей. Чтобы создать автономный инсталляционный пакет для программ стороннего производителя, необходимо создать пользовательский инсталляционный пакет.

Убедитесь, что автономный инсталляционный пакет не доступен для третьих лиц.

Чтобы создать автономный инсталляционный пакет:

1. Выполните одно из следующих действий:
   - Перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Инсталляционные пакеты**.
   - 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 данной программой**, если требуется установить Агент администрирования совместно с выбранной программой.

   По умолчанию параметр включен. Рекомендуется включить этот параметр, если вы не уверены, установлен ли на устройстве Агент администрирования. Если Агент администрирования уже установлен на устройстве, после установки автономного инсталляционного пакета с Агентом администрирования, Агент администрирования будет обновлен до более новой версии.

   Если вы выключите этот параметр, Агент администрирования не будет установлен на устройство, и устройство не будет управляемым.

Если автономный инсталляционный пакет для выбранной программы уже существует на Сервере администрирования, мастер отобразит сообщение об этом. В этом случае вы должны выбрать одно из следующих действий:

- **Создать автономный инсталляционный пакет**. Выберите этот параметр, например, если вы хотите создать автономный инсталляционный пакет для новой версии программы, и чтобы также остался автономный инсталляционный пакет для предыдущей версии программы, который вы создали ранее. Новый автономный инсталляционный пакет расположен в другой папке.
- **Использовать существующий автономный инсталляционный пакет**. Выберите этот параметр, если вы хотите использовать существующий автономный инсталляционный пакет. Процесс создания пакета не запускается.
- **Сформировать заново существующий автономный инсталляционный пакет**. Выберите этот параметр, если хотите создать автономный инсталляционный пакет для этой же программы еще раз. Автономный инсталляционный пакет размещается в той же папке.

5. На шаге **Перемещение в список управляемых устройств** параметр **Не перемещать устройства** выбран по умолчанию. 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 **Перемещать нераспределенные устройства в эту группу** и укажите группу администрирования, в которую вы хотите переместить клиентское устройство. По умолчанию устройства перемещаются в группу **Управляемые устройства**.

6. 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. Вы можете просмотреть список автономных инсталляционных пакетов, нажав на кнопку **Просмотреть список автономных пакетов**, расположенную над списком инсталляционных пакетов.

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:

Нажмите на кнопку **Просмотреть список автономных пакетов**.

Свойства автономных инсталляционных пакетов в списке отображаются следующим образом:

- **Имя пакета**. Имя автономного инсталляционного пакета, которое автоматически формируется из имени и версии программы, включенной в пакет.
- **Название программы**. Имя программы, которая включена в автономный инсталляционный пакет.
- **Версия программы**.
- **Имя инсталляционного пакета Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Версия Агента администрирования**. Параметр отображается только в том случае, если в автономный инсталляционный пакет включен Агент администрирования.
- **Размер**. Размер файла (МБ).
- **Группа**. Имя группы, в которую перемещается клиентское устройство после установки Агента администрирования.
- **Создан**. Дата и время создания автономного инсталляционного пакета.
- **Изменен**. Дата и время изменения автономного инсталляционного пакета.
- **Путь**. Полный путь к папке, в которой находится автономный инсталляционный пакет.
- **Веб-адрес**. Веб-адрес расположения автономного инсталляционного пакета.
- **Хеш файла**. Параметр используется для подтверждения того, что автономный инсталляционный пакет не был изменен третьими лицами, и у пользователя есть тот же файл, который вы создали и передали пользователю.

Чтобы просмотреть список автономных инсталляционных пакетов для определенного инсталляционного пакета,

выберите инсталляционный пакет в списке и над списком нажмите на кнопку **Просмотреть список автономных пакетов**.

В списке автономных инсталляционных пакетов вы можете сделать следующее:

- Опубликовать автономный инсталляционный пакет на Веб-сервере, с помощью кнопки **Опубликовать**. Опубликованный автономный инсталляционный пакет доступен для загрузки пользователям, которым вы отправили ссылку на автономный инсталляционный пакет.
- Отменить публикацию автономного инсталляционного пакета на Веб-сервере, нажав на кнопку **Отменить публикацию**. Неопубликованный автономный инсталляционный пакет доступен для загрузки только вам и другим администраторам.
- Загрузить автономный инсталляционный пакет на свое устройство, нажав на кнопку **Загрузить**.
- Отправить электронное письмо со ссылкой на автономный инсталляционный пакет, нажав на кнопку **Отправить по электронной почте**.
- Удалить автономный инсталляционный пакет, нажав на кнопку **Удалить**.

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 (для Ubuntu 10.04, версия Sudo 1.7.2p1 или выше).
   - Интерпретатор языка Perl версии 5.10 или выше.
2. Выполните проверку конфигурации устройства:
   a. Проверьте, что возможно подключение к устройству через SSH (например, программа PuTTY).

      Если вы не можете подключиться к устройству, откройте файл `/etc/ssh/sshd_config` и убедитесь, что следующие параметры имеют значения:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Не изменяйте файл /etc/ssh/sshd_config, если вы можете без проблем подключиться к устройству; в противном случае вы можете столкнуться с ошибкой аутентификации SSH при выполнении задачи удаленной установки.

      Сохраните файл (при необходимости) и перезапустите службу SSH, используя команду `sudo service ssh restart`.

   b. Отключите пароль запроса sudo для учетной записи пользователя, которая используется для подключения к устройству.

   c. Используйте команду sudo `visudo`, чтобы открыть конфигурационный файл sudoers.

      В открывшемся файле добавьте следующую строку в конец файла: `<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.

   Если вы хотите установить Агент администрирования на устройства с операционной системой РЕД ОС 7.3.4 и выше или МСВСфера 9.2 и выше, установите пакет libxcrypt-compat для корректной работы Агента администрирования.

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, чтобы настроить 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.

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 программы или с веб-сайта "Лаборатории Касперского".

   c. Для создания пакета удаленной установки используйте файлы:

   - klnagent.kpd;
   - akinstall.sh;
   - deb или rpm пакет Агента администрирования.

2. Создайте задачу удаленной установки программы с параметрами:

   - В окне **Параметры** мастера создания задачи установите флажок **Средствами операционной системы с помощью Сервера администрирования**. Снимите все остальные флажки.
   - На странице **Выбор учетной записи для запуска задачи** укажите параметры учетной записи, которая используется для подключения к устройству через SSH.

3. Запустите задачу удаленной установки программы. Используйте параметр для команды `su`, чтобы сохранить среду: `-m, -p, --preserve-environment`.

Установка программ с помощью задачи удаленной установки

Kaspersky Security Center Linux позволяет удаленно устанавливать программы на устройства с помощью задач удаленной установки. Задачи создаются и назначаются устройствам с помощью мастера. Чтобы быстрее и проще назначить задачу устройствам, вы можете указывать в окне мастера устройства удобным для вас способом:

- **Выбрать устройства, обнаруженные в сети Сервером администрирования**. Задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.
- **Задать адреса устройств вручную или импортировать из списка**. Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.
- **Назначить задачу выборке устройств**. В этом случае задача назначается устройствам, входящим в состав ранее созданной выборки. Вы можете указать выборку, созданную по умолчанию, или вашу собственную выборку.
- **Назначить задачу группе администрирования**. В этом случае задача назначается устройствам, входящим в ранее созданную группу администрирования.

Для правильной работы задачи удаленной установки на устройстве, на котором не установлен Агент администрирования, необходимо открыть порты TCP 139 и 445, UDP 137 и 138. Эти порты по умолчанию открыты на всех устройствах, включенных в домен. Они открываются автоматически с помощью утилиты подготовки устройств к удаленной установке.

Установка программы на выбранные устройства

Развернуть все | Свернуть все

Этот раздел содержит информацию о том, как удаленно установить программу на устройства в группе администрирования, устройства с определенными IP-адресами или набор управляемых устройств.

Чтобы установить программу на выбранные устройства:

1. В главном окне программы перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи.
3. В поле **Тип задачи** выберите **Удаленная установка программы**.
4. Выберите один из следующих вариантов:

   - **Назначить задачу группе администрирования**

     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.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.
5. Следуйте далее указаниям мастера.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы для выбранного набора устройств. Если вы выбрали параметр **Назначить задачу группе администрирования**, задача является групповой.
6. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки, выбранная программа устанавливается на указанный набор устройств.

Установка программ на подчиненные Серверы администрирования

Чтобы установить программу на подчиненные Серверы администрирования:

1. Подключитесь к Серверу администрирования, под управлением которого находятся нужные вам подчиненные Серверы администрирования.
2. Убедитесь в том, что соответствующий устанавливаемой программе инсталляционный пакет находится на каждом из выбранных подчиненных Серверов администрирования. Если вы не можете найти инсталляционный пакет ни на одном из подчиненных Серверов, распространите его. Для этого создайте задачу с типом задачи **Распространение инсталляционного пакета**.
3. Создайте задачу удаленной установки программы на подчиненных Серверах администрирования. Выберите тип задачи **Удаленная установка программы на подчиненный Сервер администрирования**.

   В результате работы мастера создания задачи будет создана задача удаленной установки выбранной программы на выбранные подчиненные Серверы администрирования.
4. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

После выполнения задачи удаленной установки выбранная программа устанавливается на подчиненные Серверы администрирования.

Указание параметров удаленной установки на устройствах под управлением Unix

Развернуть все | Свернуть все

Когда вы устанавливаете программу на устройство под управлением Unix с помощью задачи удаленной установки, вы можете указать параметры, специфичные для Unix, для этой задачи. Эти параметры доступны в свойствах задачи после ее создания.

Чтобы указать параметры, специфичные для Unix, для задачи удаленной установки:

1. В главном окне программы перейдите в раздел **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 раздел **Параметры программы** → **Параметры, специфичные для Unix**.
4. Задайте следующие параметры:

   - **Установить пароль для учетной записи root (только для развертывания через SSH)**

     Если команду `sudo` нельзя использовать на целевом устройстве без указания пароля, выберите этот параметр, а затем укажите пароль для учетной записи root. Kaspersky Security Center 14 Linux передает пароль в зашифрованном виде на целевое устройство, расшифровывает пароль, а затем запускает процедуру установки от имени учетной записи root с указанным паролем.

     Kaspersky Security Center 14 Linux не использует учетную запись или указанный пароль для создания SSH подключения.
   - **Укажите путь к временной папке с правами Выполнение на целевом устройстве (только для развертывания через SSH)**

     Если папка /tmp на целевом устройстве не имеет права Выполнение, выберите этот параметр, а затем укажите путь к папке с правами Выполнение. Kaspersky Security Center 14 Linux использует указанную папку в качестве временной папки для доступа по SSH. Программа помещает инсталляционный пакет в папку и запускает процедуру установки.
5. Нажмите на кнопку **Сохранить**.

Указанные параметры задачи сохранены.

Запуск и остановка программ "Лаборатории Касперского"

Вы можете использовать задачу *Запуск или остановка программы* для запуска и остановки программ "Лаборатории Касперского" на управляемых устройствах.

Чтобы создать задачу запуска или остановки программы:

1. В главном окне программы перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Программа** выберите программу, для которой вы хотите создать задачу.

   Программы "Лаборатории Касперского" отображаются в списке, если вы ранее добавили веб-плагины управления этих программ.
4. В списке **Тип задачи** выберите задачу **Активация программы**.
5. В поле **Название задачи** укажите название новой задачи.

   Название задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
6. Выберите устройства, которым будет назначена задача.
7. В окне **Программы** выполните следующее:

   - Установите флажки рядом с названиями программ, для которых вы хотите создать задачу.
   - Выберите параметр **Запустить программу** или **Остановить программу**.
8. 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.
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 и сохраните параметры.

Задача создана и настроена.

Если вы хотите запустить задачу, выберите задачу в списке задач и нажмите на кнопку **Запустить**.

Замещение программ безопасности сторонних производителей

Для установки программ безопасности "Лаборатории Касперского" средствами Kaspersky Security Center Linux может потребоваться удалить стороннее программное обеспечение, несовместимое с устанавливаемой программой. Kaspersky Security Center предоставляет несколько способов удаления программ сторонних производителей.

Удаление несовместимых программ при настройке удаленной установки программы

Вы можете включить параметр **Удалять несовместимые программы автоматически** во время настройки удаленной установки программы безопасности в мастере развертывания защиты. Если этот параметр включен, Kaspersky Security Center удаляет несовместимые программы перед установкой программы безопасности на управляемое устройство.

Инструкции: Удаление несовместимых программ перед установкой.

Удаление несовместимых программ с помощью отдельной задачи

Для удаления несовместимых программ используется задача **Удаленная деинсталляция программы**. Задачу следует запускать на устройствах перед задачей установки программы безопасности. Например, в задаче установки можно выбрать расписание типа **По завершении другой задачи**, где другой задачей является задача **Удаленная деинсталляция программы**.

Этот способ удаления целесообразно использовать в случаях, если инсталлятор программы безопасности не может успешно удалить какую-либо из несовместимых программ.

Инструкции: Создание задачи.

Удаленная деинсталляция программ или обновлений программного обеспечения

Развернуть все | Свернуть все

Вы можете удаленно деинсталлировать программы или обновления программного обеспечения на управляемых устройствах под управлением Linux только с помощью Агента администрирования.

Чтобы удаленно деинсталлировать программы или обновления программного обеспечения:

1. В главном окне программы перейдите в раздел **Устройства → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. Для программы Kaspersky Security Center выберите тип задачи **Удаленная деинсталляция программы**.
4. Укажите имя задачи, которую вы создаете.

   Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).
5. Выберите устройства, которым будет назначена задача.
6. Выберите, какую программу вы хотите деинсталлировать, а затем выберите требуемые программы, обновления или патчи, которые вы хотите удалить:

   - **Удалить управляемую программу**

     Отображается список программ "Лаборатории Касперского". Выберите программу, которую вы хотите деинсталлировать.

   - **Удалить несовместимую программу**

     Отобразится список программ, несовместимых с программами безопасности "Лаборатории Касперского" или с Kaspersky Security Center. Установите флажки напротив программ, которые требуется удалить.

   - **Удалить программу из реестра программ**

     По умолчанию Агенты администрирования отправляют на Сервер администрирования информацию о программах, установленных на управляемых устройствах. Список установленных программ хранится в реестре программ.

     Чтобы выбрать программу из реестра программ:

a. Нажмите на поле **Программа для деинсталляции** и выберите программу, которую вы хотите деинсталлировать.

Если вы выбрали Агент администрирования Kaspersky Security Center, при запуске задачи статус *Завершено успешно* показывает, что процесс удаления запущен. При удалении Агента администрирования Kaspersky Security Center статус не меняется. В случае сбоя задачи статус меняется на *Сбой*.

b. Укажите параметры деинсталляции:

- Способ удаления

  Выберите, как вы хотите деинсталлировать программу:

  - **Автоматически определять команду удаления**

    Если у программы есть команда деинсталляции, заданная поставщиком программы, Kaspersky Security Center использует эту команду. Рекомендуется выбрать этот вариант.

  - **Задать команду удаления**

    Выберите этот вариант, если вы хотите указать свою команду для деинсталляции программы.

    Рекомендуется сначала попробовать деинсталлировать программу с помощью параметра **Автоматически определять команду удаления**. Если деинсталляция с помощью автоматически определенной команды не удалась, используйте свою команду.

    Введите команду установки в это поле и укажите следующий параметр:

    Используйте эту команду для удаления, только если команда по умолчанию не была обнаружена автоматически

    Kaspersky Security Center проверяет, есть ли у выбранной программы команда деинсталляции, заданная поставщиком программы. Если команда найдена, Kaspersky Security Center будет использовать ее вместо команды, указанной в поле **Команда для удаления программы**.

    Рекомендуется включать этот параметр.

- Считать, что требуется перезагрузка после успешного удаления

  Если после деинсталляции программы требуется перезагрузка операционной системы на управляемом устройстве, операционная система перезагружается автоматически.

7. Укажите, как клиентские устройства будут загружать утилиту удаления:

- С помощью Агента администрирования

  Файлы доставляются на клиентские устройства Агентом администрирования, установленным на этих клиентских устройствах.

  Если этот параметр выключен, файлы доставляются с помощью инструментов операционной системы Linux.

  Рекомендуется включить этот параметр, если задача назначена для устройств с установленными Агентами администрирования.

- Средствами операционной системы с помощью Сервера администрирования

  Параметр устарел. Используйте параметр **С помощью Агента администрирования** или **Средствами операционной системы с помощью точек распространения** вместо этого параметра.

  Файлы передаются на клиентские устройства с использованием средств операционной системы 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.

- Средствами операционной системы с помощью точек распространения

  Файлы передаются на клиентские устройства с использованием инструментов операционной системы с помощью точек распространения. Этот параметр можно включить, 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.

- **Максимальное количество одновременных загрузок**

  Максимально допустимое количество клиентских устройств, на которые Сервер администрирования может одновременно передавать файлы. Чем больше это число, тем быстрее будет деинсталлирована программа, но нагрузка на Сервер администрирования увеличивается.

- **Максимальное количество попыток деинсталляции**

  Если при запуске задачи *Удаленная деинсталляция программы* не удается деинсталлировать программу с управляемого устройства за указанное в параметрах количество запусков установок, Kaspersky Security Center прекращает доставку утилиты деинсталляции на это управляемое устройство и больше не запускает установщик на устройстве.

  Параметр **Максимальное количество попыток деинсталляции** позволяет вам сохранить ресурсы управляемого устройства, а также уменьшить трафик (деинсталляция, запуск файла MSI и сообщения об ошибках).

  Повторяющиеся попытки запуска задачи могут указывать на проблему на устройстве, которая препятствует деинсталляции. Администратор должен решить проблему за указанное количество попыток деинсталляции и перезапустить задачу (вручную или по расписанию).

  Если удаление не выполнено, проблема будет считаться неразрешимой и любые дальнейшие запуски считаются дорогостоящими с точки зрения нежелательного расхода ресурсов и трафика.

  После создания задачи, количество попыток установки равно `0`. Каждый запуск установки, который возвращает ошибку на устройстве, увеличивает показания счетчика.

  Если количество попыток деинсталляции, указанное в параметрах задачи, было превышено и устройство готово к деинсталляции программы, вы можете увеличить значение параметра **Максимальное количество попыток деинсталляции** и запустить задачу деинсталляции программы. Также вы можете создать другую задачу *Удаленная деинсталляция программы*.

- **Предварительно проверять тип операционной системы перед загрузкой**

  Перед передачей файлов на клиентские устройства Kaspersky Security Center проверяет, применимы ли параметры утилиты установки к операционной системе клиентского устройства. Если параметры не применимы, Kaspersky Security Center не передает файлы и не пытается установить программу. Например, чтобы установить некоторые программы с устройств группы администрирования, в которую входят устройства с различными операционными системами, вы можете назначить задачу установки группе администрирования, а затем включить этот параметр, чтобы пропускать устройства с операционной системой, отличной от требуемой.

8. Укажите параметры перезагрузки операционной системы:

- **Не перезагружать устройство**

  Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

- **Перезагрузить устройство**

  В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- **Принудительно закрывать программы в заблокированных сеансах**

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

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

9. Если необходимо, добавьте учетные записи, которые будут использоваться для запуска задачи удаленной деинсталляции:

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

  Если выбран этот вариант, не требуется указывать учетную запись, от имени которой будет запускаться инсталлятор программы. Задача запускается под учетной записью, под которой работает служба Сервера администрирования.

  Если Агент администрирования не установлен на клиентских устройствах, вариант недоступен.

- **Учетная запись требуется (Агент администрирования не используется)**

  Выберите этот вариант, если Агент администрирования не установлен на устройствах, для которых вы назначаете задачу *Удаленная деинсталляция программы*. В этом случае вы можете указать учетную запись пользователя или SSH-сертификат для деинсталляции программы.

  - **Локальная учетная запись**. Если выбран этот вариант, укажите учетную запись пользователя, от имени которой будет запускаться инсталлятор программы. Нажмите на кнопку **Добавить**, выберите **Локальная учетная запись** и укажите 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.

  - **SSH сертификат**. Если вы хотите деинсталлировать программу с клиентского устройства под управлением Linux, вы можете указать SSH-сертификат вместо учетной записи пользователя. Нажмите на кнопку **Добавить**, выберите **SSH сертификат** и укажите закрытый и открытый ключи сертификата.

    Чтобы сгенерировать закрытый ключ, вы можете использовать утилиту ssh-keygen. Обратите внимание, что Kaspersky Security Center поддерживает формат закрытых ключей PEM, а утилита ssh-keygen по умолчанию генерирует SSH-ключи в формате OPENSSH. Формат OPENSSH не поддерживается Kaspersky Security Center. Чтобы создать закрытый ключ в поддерживаемом формате PEM, добавьте параметр -m PEM в команду ssh-keygen.

    Например:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< электронная почта пользователя >"
    ```

10. 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.

11. Нажмите на кнопку **Готово**.

    Задача будет создана и отобразится в списке задач.

12. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.

13. В окне свойств задачи укажите общие параметры задачи.

14. Нажмите на кнопку **Сохранить**.

15. Запустите задачу вручную или дождитесь ее запуска в соответствии с расписанием, указанным вами в параметрах задачи.

В результате выполнения задачи удаленной деинсталляции выбранная программа будет удалена с выбранных устройств.

Ограничения удаленной деинсталляции

Иногда удаленная деинсталляция программ сторонних производителей может завершится предупреждением: "Удаление на этом устройстве завершено с предупреждениями: Программа для деинсталляции не установлена". Эта проблема возникает, когда программа для деинсталляции, уже была деинсталлирована или была установлена только для одного пользователя. Программы, установленные для одного пользователя (далее также "программы для каждого пользователя"), становятся невидимыми и не могут быть деинсталлированы удаленно, если пользователь не вошел в систему.

Такое поведение отличается от поведения программ, предназначенных для использования несколькими пользователями на одном устройстве (далее также "программы устройства"). Программы для каждого устройства видны и доступны всем пользователям этого устройства.

Поэтому программы для каждого пользователя должны быть деинсталлированы только когда пользователь вошел в систему.

Источники информации об установленных программах

Агент администрирования получает информацию о программном обеспечении, установленном на устройствах Windows, из следующих ключей реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о программах, установленных для всех пользователей.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о программах, установленных для всех пользователей.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о программах, установленных для текущего пользователя.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Содержит информацию о программах, установленных для набора пользователей.

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.

Программы "Лаборатории Касперского": лицензирование и активация

В этом разделе описаны возможности Kaspersky Security Center по работе с лицензионными ключами управляемых программ "Лаборатории Касперского".

Kaspersky Security Center Linux позволяет централизованно распространять лицензионные ключи программ "Лаборатории Касперского" на клиентские устройства, наблюдать за использованием ключей и продлевать сроки действия лицензий.

При добавлении лицензионного ключа с помощью Kaspersky Security Center свойства лицензионного ключа сохраняются на Сервере администрирования. На основании этой информации программа формирует отчет об использовании лицензионных ключей и уведомляет администратора об истечении сроков действия лицензий и о превышении лицензионных ограничений, заложенных в свойствах лицензионных ключей. Вы можете настраивать параметры оповещений об использовании лицензионных ключей в составе параметров Сервера администрирования.

Лицензирование управляемых программ

Программы "Лаборатории Касперского" установленные на управляемых устройствах, должны быть активированы путем применения файла ключа или кода активации к каждой из программ. Файл ключа или код активации может быть распространен следующими способами:

- автоматическое распространение;
- с помощью инсталляционного пакета управляемой программы;
- с помощью задачи добавления лицензионного ключа управляемой программы;
- активация управляемой программы вручную.

Вы можете добавить активный или резервный лицензионный ключ любым из перечисленных выше способов. Программа "Лаборатории Касперского" использует активный в данный момент ключ и сохраняет резервный ключ, который будет применяться после истечения срока действия активного ключа. Программа, для которого вы добавляете лицензионный ключ, определяет, является ли ключ активным или резервным. Определение ключа не зависит от способа, который вы используете для добавления лицензионного ключа.

Автоматическое распространение

Если вы используете разные управляемые программы и вам важно распространить определенный файл ключ или код активации на устройства, используйте другие способы распространения кода активации или ключа.

Kaspersky Security Center позволяет автоматически распространять имеющиеся лицензионные ключи на устройства. Например, в хранилище Сервера администрирования находится три лицензионных ключа. Вы должны включить параметр **Автоматически распространяемый лицензионный ключ** для всех трех лицензионных ключей. На устройствах организации установлена программа безопасности "Лаборатории Касперского", например, Kaspersky Endpoint Security для Linux. Обнаружено новое устройство, на которое необходимо распространить лицензионный ключ. Программа определяет, что для этого устройства подходит, например, два лицензионных ключа из хранилища, лицензионный ключ *Ключ_1*и лицензионный ключ *Ключ_2*. На устройство распространяется один из подходящих лицензионных ключей. В этом случае нельзя предсказать, какой из этих двух лицензионных ключей будет распространен на данное устройство, так как автоматическое распространение лицензионных ключей не предполагает вмешательства администратора.

При распространении лицензионного ключа на устройства происходит подсчет устройств для данного лицензионного ключа. Вам необходимо удостовериться, что количество устройств, на которые распространяется лицензионный ключ, не превышает лицензионное ограничение. В случае если количество устройств превышает лицензионное ограничение, 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
- Автоматическое распространение лицензионного ключа

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для программы.
- 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 управляемой программы.

Из соображений безопасности не рекомендуется использовать этот параметр. Файл ключа или код активации, добавленный в инсталляционный пакет, может быть скомпрометирован.

В случае установки управляемой программы с помощью инсталляционного пакета вы можете указать код активации или файл ключа в инсталляционном пакете или в политике этой программы. Лицензионный ключ распространится на управляемые устройства при очередной синхронизации устройства с Сервером администрирования.

Инструкции: Добавление лицензионного ключа в инсталляционный пакет.

Распространение с помощью задачи добавления лицензионного ключа управляемой программы

В случае использования задачи добавления лицензионного ключа управляемой программы вы можете выбрать лицензионный ключ, который необходимо распространить на устройства, и выбрать устройства удобным вам способом, например, выбрав группу администрирования или выборку устройств.

Перед распространением файл ключа или код активации необходимо добавить в хранилище Сервера администрирования.

Инструкции:

- Добавление лицензионного ключа в хранилище Сервера администрирования
- Распространение лицензионного ключа на клиентские устройства

Добавление кода активации или файла ключа вручную на устройства.

Вы можете активировать установленную программу "Лаборатории Касперского" локально, используя инструменты программы. Дополнительную информацию см. в документации к установленным программам.

Добавление лицензионного ключа в хранилище Сервера администрирования

Чтобы добавить лицензионный ключ в хранилище Сервера администрирования:

1. В главном окне программы перейдите в раздел **Операции → 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.

Распространение лицензионного ключа на клиентские устройства

Kaspersky Security Center 14 Web Console позволяет распространить лицензионный ключ на клиентские устройства автоматически или с помощью задачи добавления лицензионного ключа.

Перед распространением добавьте лицензионный ключ в хранилище Сервера администрирования.

Чтобы распространить лицензионный ключ на клиентские устройства с помощью задачи добавления ключа:

1. В главном окне программы перейдите в раздел **Устройства → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится **мастер создания задачи**. Для продолжения работы мастера нажмите на кнопку **Далее**.
3. В раскрывающемся списке **Программа** выберите программу, для которой 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.
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 **Закрыть**.

     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 ключа.

     c. Нажмите на кнопку **Закрыть**.

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** снимите флажок **Использовать по умолчанию в качестве резервного лицензионного ключа**, если вы хотите заменить действующий активный лицензионный ключ.

    Например, это необходимо, когда организация меняется и на устройстве требуется ключ другой организации или если ключ был перевыпущен и срок действия новой лицензии истекает раньше, чем срок действия текущей лицензии. Чтобы избежать ошибок, снимите флажок **Использовать как резервный лицензионный ключ**.

    Если вы хотите узнать больше о проблемах, которые могут возникнуть при добавлении лицензионного ключа в Kaspersky Security Center, и способах их решения, обратитесь к Базе знаний Kaspersky Security Center.

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.

    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.

После завершения задачи, лицензионный ключ распространится на выбранные устройства.

Автоматическое распространение лицензионного ключа

Kaspersky Security Center Linux позволяет автоматически распространять на управляемые устройства лицензионные ключи, размещенные в хранилище ключей на Сервере администрирования.

Чтобы автоматически распространять лицензионный ключ на управляемые устройства:

1. В главном окне программы перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.

2. Нажмите на имя лицензионного ключа, который вы хотите автоматически распространять на устройства.

3. В открывшемся окне свойств лицензионного ключа установите флажок **Автоматически распространять лицензионный ключ на управляемые устройства**.

4. Нажмите на кнопку **Сохранить**.

Лицензионный ключ будет автоматически распространяться на те устройства, для которых он подходит.

Распространение лицензионного ключа выполняется средствами Агента администрирования. Задачи распространения резервного лицензионного ключа для программы при этом не создаются.

При автоматическом распространении лицензионного ключа учитывается лицензионное ограничение на количество устройств. Лицензионное ограничение задано в свойствах лицензионного ключа. Если лицензионное ограничение достигнуто, распространение лицензионного ключа на устройства автоматически прекращается.

Обратите внимание, что автоматически распространяемый лицензионный ключ может не отображаться в хранилище виртуального Сервера администрирования в следующих случаях:

- Лицензионный ключ недействителен для программы.
- 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 установлен флажок **Автоматически распространять лицензионный ключ на управляемые устройства** в окне свойств лицензионного ключа, лицензионный ключ будет немедленно распространен в вашей сети. Если вы не выберете этот параметр, вы можете использовать задачу распространения лицензионного ключа позже.

Автоматическое распространение лицензионных ключей, настроенных на главном Сервере администрирования, не включает устройства, управляемые невиртуальными подчиненными Серверами администрирования.

Просмотр информации об используемых лицензионных ключах

Чтобы просмотреть список лицензионных ключей, добавленных в хранилище Сервера администрирования:

В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.

Отобразится список файлов ключей и кодов активации, добавленных в хранилище Сервера администрирования.

Чтобы просмотреть подробную информацию о лицензионном ключе:

1. В главном окне программы перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Нажмите на имя требуемого лицензионного ключа.

В открывшемся окне свойств лицензионного ключа вы можете просмотреть:

- На закладке **Общие** – основную информацию о лицензионном ключе.
- На закладке **Устройства** – список клиентских устройств, на которых использовался лицензионный ключ для активации установленной программы "Лаборатории Касперского".

Чтобы просмотреть, какие лицензионные ключи распространены на выбранное клиентское устройство:

1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Нажмите на имя требуемого устройства.
3. В открывшемся окне свойств устройства выберите закладку **Программы**.
4. Нажмите на название программы, для которой вы хотите просмотреть информацию о распространенном лицензионном ключе.
5. В открывшемся окне свойств программы перейдите на закладку **Общие** и откройте раздел **Лицензия**.

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.

Удаление лицензионного ключа из хранилища

При удалении активного лицензионного ключа, который распространен на управляемые устройства, программы продолжают работать на управляемых устройствах.

Чтобы удалить файл ключа или код активации из хранилища Сервера администрирования:

1. Перейдите в раздел **Операции** → **Лицензирование** → **Лицензии "Лаборатории Касперского"**.
2. Выберите файл ключа или код активации, который вы хотите удалить из хранилища.
3. Нажмите на кнопку **Удалить**.

4. Нажмите на кнопку **OK** для подтверждения выполнения операции.

Выбранный файл ключа или код активации удален из хранилища.

Можно добавить удаленный лицензионный ключ повторно или добавить другой лицензионный ключ.

Отзыв согласия с Лицензионным соглашением

Если вы решите прекратить защиту некоторых своих клиентских устройств, вы можете отозвать Лицензионное соглашение для любой управляемой программы "Лаборатории Касперского". Вам нужно удалить выбранную программу, прежде чем отзывать ее Лицензионное соглашение.

Чтобы отозвать Лицензионное соглашение для управляемых программ "Лаборатории Касперского":

1. Откройте окно свойств Сервера администрирования и на закладке **Общие** выберите раздел **Лицензионные соглашения**.

   Отобразится список Лицензионных соглашений, принятых при создании инсталляционных пакетов, установке обновлений или развертывании Kaspersky Security для мобильных устройств.

2. В списке выберите Лицензионные соглашения, которые вы хотите отозвать.

   Можно просмотреть следующие свойства Лицензионных соглашений:

   - Дата принятия Лицензионного соглашения.
   - Имя пользователя, принявшего Лицензионное соглашение.

3. Нажмите на дату принятия любого Лицензионного соглашения, чтобы открыть окно его свойств, в котором отображаются следующие данные:

   - Имя пользователя, принявшего Лицензионное соглашение.
   - Дата принятия Лицензионного соглашения.
   - Уникальный идентификатор (UID) Лицензионного соглашения.
   - Полный текст Лицензионного соглашения.
   - Список объектов (инсталляционных пакетов, обновлений, мобильных приложений), связанных с Лицензионным соглашением, и их соответствующие имена и типы.

4. В нижней части окна свойств Лицензионного соглашения нажмите на кнопку **Отозвать Лицензионное соглашение**.

   Если существуют какие-либо объекты (инсталляционные пакеты и их соответствующие задачи), которые не позволяют отозвать Лицензионное соглашение, отображается соответствующее уведомление. Вы не можете продолжить отзыв, пока не удалите эти объекты.

   В открывшемся окне отобразится сообщение о том, что сначала необходимо удалить программу "Лаборатории Касперского", которой соответствует это Лицензионное соглашение.

5. Нажмите на кнопку, подтверждающую отзыв лицензии.

Лицензионное соглашение отозвано. Лицензионное соглашение больше не отображается в списке Лицензионных соглашений в разделе **Лицензионные соглашения**. Окно свойств Лицензионного соглашения закрывается; программа больше не установлена.

Продление срока действия лицензии программ "Лаборатории Касперского"

Вы можете продлить срок действия лицензии программ "Лаборатории Касперского", срок действия которой истек или скоро истечет (менее чем через 30 дней).

Чтобы продлить лицензии срок действия истекает или уже истек:

1. Выполните одно из следующих действий:

   - В главном окне программы перейдите в раздел **Операции → Лицензирование → Лицензии "Лаборатории Касперского"**.
   - В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга** и перейдите по ссылке **Просмотреть лицензии, срок действия которых истек** рядом с уведомлением.

   Откроется окно **Лицензии "Лаборатории Касперского"**, в котором вы можете просмотреть и продлить срок действия лицензии.

2. Перейдите по ссылке **Продлить срок действия лицензии** 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 14 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.

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 14 Linux 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 службы.
  - **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 программы 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.

Настройка защиты сети

В этом разделе содержится информация о настройке вручную политик и задач, о ролях пользователей, о построении структуры групп администрирования и об иерархии задач.

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.
- Установили Kaspersky Security Center 14 Web Console.
- Основной сценарий установки Kaspersky Security Center завершен.
- Мастер первоначальной настройки завершен или следующие политики и задачи созданы вручную в группе администрирования **Управляемые устройства**:
  - политика Kaspersky Endpoint Security;
  - групповая задача обновления Kaspersky Endpoint Security;
  - политика Агента администрирования.

Настройка защиты сети состоит из следующих этапов:

1. **Настройка и распространение политик и профилей политик для программ "Лаборатории Касперского"**

   Для настройки и распространения параметров программ "Лаборатории Касперского", установленных на управляемых устройствах, можно использовать два различных подхода управления безопасностью: ориентированный на пользователей и ориентированный на устройства. Можно комбинировать эти два подхода.

2. **Настройка задач для удаленного управления программами "Лаборатории Касперского"**

   Проверьте задачи, созданные с помощью мастера первоначальной настройки, и при необходимости оптимизируйте их параметры.

   Инструкции: Настройка групповой задачи обновления Kaspersky Endpoint Security.

   При необходимости создайте дополнительные задачи управления программами "Лаборатории Касперского", установленными на клиентских устройствах.

3. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых программ, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции: Настройка количества событий в хранилище событий.

Результаты

После завершения этого сценария ваша сеть будет защищена благодаря настройке программ "Лаборатории Касперского", задач и событий, получаемых Сервером администрирования:

- Программы "Лаборатории Касперского" настроены в соответствии с политиками и профилями политик.
- Управление программами осуществляется с помощью набора задач.
- Задано максимальное количество событий, которые могут храниться в базе данных.

После завершения настройки защиты сети вы можете приступить к настройке регулярных обновлений баз и программ "Лаборатории Касперского".

Подходы к управлению безопасностью, ориентированные на устройства и на пользователей

Вы можете управлять параметрами безопасности с позиции функций устройства и с позиции пользовательских ролей. Первый подход называется *управление безопасностью, ориентированное на устройства*, второй подход называется *управление безопасностью, ориентированное на пользователей*. Чтобы применить разные параметры программ к разным устройствам, вы можете использовать один или оба типа управления в комбинации.

Управление безопасностью, ориентированное на устройства, позволяет вам применять различные параметры программы безопасности к управляемым устройствам в зависимости от особенностей устройства. Например, вы можете применить различные параметры к устройствам, которые размещены в разных группах администрирования.

Управление безопасностью, ориентированное на пользователя, позволяет вам применять различные параметры программ безопасности к различным ролям пользователей. Вы можете создать несколько пользовательских ролей, назначить соответствующую пользовательскую роль каждому пользователю и определить различные параметры программы для устройств, принадлежащих пользователям с различными ролями. Например, можно применить различные параметры программ к устройствам бухгалтеров и к устройствам специалистов отдела кадров. В результате внедрения управления безопасностью, ориентированного на пользователей, каждый отдел – отдел бухгалтерии и отдел кадров – получит свою собственную конфигурацию параметров для работы с программами "Лаборатории Касперского". Конфигурация параметров определяет, какие параметры программы могут быть изменены пользователями, а какие принудительно установлены и заблокированы администратором.

Управление безопасностью, ориентированное на пользователей, позволяет применять заданные параметры программ для отдельных пользователей. Это может потребоваться, если сотруднику назначена уникальная роль в организации или если требуется проконтролировать инциденты безопасности, связанные с определенным сотрудником. В зависимости от роли этого сотрудника в компании, можно расширить или сократить его права, чтобы изменить параметры программы. Например, может потребоваться расширить права системного администратора, управляющего клиентскими устройствами в локальном офисе.

Вы также можете комбинировать подходы к управлению безопасностью, ориентированные на пользователей и ориентированные на устройства. Например, можно настроить разные политики для каждой группы администрирования, а затем дополнительно создать профили политик 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 приоритетом профилей политик.
3. Политики модифицируются профилями политик, связанными с ролями пользователей.

Настройка и распространение политик: подход, ориентированный на устройства

После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на пользователей как альтернативу или дополнительную возможность для подхода, ориентированного на устройства. Узнайте больше о двух подходах к управлению.

Этапы

Сценарий управления программами "Лаборатории Касперского", ориентированный на устройства, содержит следующие шаги:

1 Настройка политик программ

Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждой программы. Этот набор политик будет применен к клиентским устройствам.

При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для Kaspersky Endpoint Security для Linux. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы.

Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. 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.

2 Создание профилей политики (если требуется)

Если вы хотите, чтобы к устройствам из одной группы администрирования применялись разные параметры политики, создайте профили политики 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 с определенной конфигурацией программного обеспечения или с заданными теги. Используйте теги для фильтрации устройств, соответствующих определенным критериям. Например, вы можете создать тег *CentOS*, назначить его всем устройствам под управлением операционной системы CentOS, а затем указать этот тег в правилах активации профиля политики. В результате на устройствах под управлением операционной системы CentOS установленные программы "Лаборатории Касперского" будут управляться своим профилем политики.

Инструкции:

- Создание профиля политики
- Создание правила активации профиля политики

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 программам "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация.

Результаты

После завершения сценария, ориентированного на устройства, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик.

Политики программ и профили политик будут автоматически применяться к новым устройствам, добавленным в группы администрирования.

Настройка и распространение политик: подход, ориентированный на пользователя

В этом разделе описывается сценарий, ориентированный на пользователя для централизованной настройке программ "Лаборатории Касперского", установленных на управляемых устройствах. После завершения этого сценария программы будут настроены на всех управляемых устройствах в соответствии с политиками программ и профилями политики, которые вы определяете.

Предварительные требования

Убедитесь, что вы успешно установили Сервер администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console и завершили основной сценарий развертывания. Возможно, вы также захотите рассмотреть управление безопасностью, ориентированное на устройства как альтернативу или дополнительную возможность для подхода, ориентированного на пользователя. Узнайте больше о двух подходах к управлению.

Процесс

Сценарий управления программами "Лаборатории Касперского", ориентированный на пользователя, содержит следующие шаги:

1. **Настройка политик программ**

   Настройте параметры установленных программ "Лаборатории Касперского" на управляемых устройствах с помощью создания политики для каждой программы. Этот набор политик будет применен к клиентским устройствам.

   При настройке защиты сети с помощью мастера первоначальной настройки Kaspersky Security Center создает политику по умолчанию для Kaspersky Endpoint Security. Если вы завершили процесс настройки с помощью этого мастера, вам не нужно создавать новую политику для этой программы.

   Если у вас иерархическая структура нескольких Серверов администрирования и/или групп администрирования, подчиненные Серверы администрирования и дочерние группы администрирования наследуют политики от главного Сервера администрирования по умолчанию. Вы можете принудительно наследовать параметры дочерними группами и подчиненными Серверами администрирования, чтобы запретить любые изменения параметров политик вниз по иерархии. Если вы хотите разрешить наследовать только часть параметров, вы можете заблокировать их выше по иерархии политики. 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.

2. **Укажите пользователей в качестве владельцев устройств**

   Назначьте управляемым устройствам соответствующих пользователей.

Инструкция: Назначение пользователя владельцем устройства.

3. **Определение пользовательских ролей, типичных для вашей организации**

   Подумайте о различных видах работ, которые обычно выполняют сотрудники вашей организации. Вы должны разделить всех сотрудников в соответствии с их ролями. Например, вы можете разделить их по отделам, профессиям или должностям. После этого вам потребуется создать роль пользователя для каждой группы. В этом случае каждая пользовательская роль будет иметь свой собственный профиль политики, содержащий параметры программы, специфичные для этой роли.

4. **Создание пользовательских ролей**

   Создайте и настройте пользовательскую роль для каждой группы сотрудников, которую вы определили на предыдущем шаге, или используйте предопределенные роли. Роли пользователей содержат набор прав доступа к функциям программы.

   Инструкция: Создание роли пользователя.

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.

6. **Создание профиля политики**

   Создайте профиль политики для каждой роли пользователя вашей организации. Профили политики определяют, какие параметры должны применяться к программам, установленным на устройствах пользователей, в зависимости от роли каждого пользователя.

   Инструкция: Создание профиля политики.

7. **Связь профиля политики с ролями пользователей**

   Свяжите профили политики с ролями пользователей. После чего, профиль политики становится активным для пользователей, которым определена эта роль. Параметры профиля политики, применяются к программам "Лаборатории Касперского", установленным на устройствах пользователя.

   Инструкции: Связь профилей политики с ролями.

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 программам "Лаборатории Касперского".

   Вы можете проверить, доставлены ли политики и профили политик на устройство. Kaspersky Security Center определяет дату и время доставки в свойствах устройства.

   Инструкции: Принудительная синхронизация.

Результаты

После завершения сценария, ориентированного на пользователя, программы "Лаборатории Касперского" будут настроены в соответствии с параметрами, указанными и распространенными через иерархию политик и профили политик.

Для нового пользователя вам необходимо создать учетную запись, назначить пользователю одну из созданных пользовательских ролей и назначить устройства пользователю. Политики программ и профили политик будут автоматически применяться к устройствам этого пользователя.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Оптимальный и рекомендуемый вариант расписания для Kaspersky Endpoint Security **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Параметры политики Агента администрирования

Развернуть все | Свернуть все

Чтобы настроить параметры политики Агента администрирования:

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Нажмите на название политики Агента администрирования.

   Откроется окно свойств политики Агента администрирования.

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 родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.

  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

На этой закладке можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности в следующих разделах на закладке **Настройка событий**:

- **Отказ функционирования**
- **Предупреждение**
- **Информационное сообщение**

В каждом разделе в списке 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 **Произошел инцидент**. Такие события могут произойти, например, когда свободное место на диске точки распространения меньше 2 ГБ (для установки программ и удаленной загрузки обновлений требуется не менее 4 ГБ). Чтобы настроить событие **Произошел инцидент**, нажмите на него и укажите, где хранить произошедшие события и как о них уведомлять.

Если Агент администрирования обнаружил инцидент, вы можете управлять этим инцидентом с помощью параметров управляемого устройства.

Параметры программы

Параметры

В разделе **Параметры** можно настроить параметры политики Агента администрирования:

- **Максимальный размер очереди событий (МБ)**

  В поле можно указать максимальное место на диске, которое может занимать очередь событий.

  По умолчанию указано значение 2 МБ.

- **Программа может получать расширенные данные политики на устройстве**

  Агент администрирования, установленный на управляемом устройстве, передает информацию о применяемой политике в программу безопасности (например, Kaspersky Endpoint Security для Linux). Передаваемая информация отображается в интерфейсе программы безопасности.

  Агент администрирования передает следующую информацию:

  - время доставки политики на управляемое устройство;
  - имя активной политики и политики для автономных пользователей в момент доставки политики на управляемое устройство;
  - имя и полный путь группы администрирования, которой принадлежит управляемое устройство на момент доставки политики на управляемое устройство;
  - список активных профилей политики.

    Вы можете использовать эту информацию, чтобы обеспечить применение правильной политики к устройству и в целях устранения неполадок. По умолчанию параметр выключен.

Хранилища

В разделе **Хранилища** можно выбрать типы объектов, информацию о которых Агент администрирования будет отправлять на Сервер администрирования. Если в политике Агента администрирования наложен запрет на изменение параметров, указанных в этом разделе, эти параметры недоступны для изменения.

- **Информация об установленных программах**

  Если этот параметр включен, на Сервер администрирования отправляется информация о программах, установленных на клиентских устройствах.

  По умолчанию параметр включен.

- **Информация о реестре оборудования**

  Установленный на устройстве Агент администрирования отправляет информацию об оборудовании устройства на Сервер администрирования. Вы можете просмотреть информацию об оборудовании в свойствах устройства.

  Убедитесь, что утилита lshw установлена на устройствах Linux, с которых вы хотите получить информацию об оборудовании. Сведения об оборудовании, полученные с виртуальных машин, могут быть неполными в зависимости от используемого гипервизора

Сеть

Раздел **Сеть** включает три вложенных раздела:

- **Подключения**
- **Профили соединений**
- **Расписание соединений**

В разделе **Подключения** можно настроить параметры подключения к Серверу администрирования, включить возможность использования UDP-порта и указать его номер.

- В блоке **Подключиться 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 соединения 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 Агент администрирования подключался к Серверу администрирования 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 Серверу администрирования выполняется через UDP-порт 15000.

- **Номер UDP-порта**

  В поле можно ввести номер UDP-порта. По умолчанию установлен порт 15000.

  Используется десятичная форма записи.

В подразделе **Профили соединений** раздела **Сеть** можно задать параметры сетевого местоположения и включить автономный режим, когда Сервер администрирования недоступен.

- **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. Не рекомендуется использовать этот параметр.

  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.

В группе параметров **Профили соединений** новые элементы не могут быть добавлены в список **Профили подключения к Серверу администрирования**, так как кнопка **Добавить** неактивна. Предустановленные профили соединений тоже нельзя изменить.

- **Включить автономный режим, когда Сервер администрирования недоступен**

  Если параметр включен, при подключении через этот профиль программы, установленные на клиентском устройстве, будут использовать профили политик для устройств, находящихся в автономном режиме, и политики для автономных пользователей. В случае, если для программы политика для автономных пользователей не определена, программа будет использовать активную политику.

  Если параметр выключен, программы будут использовать активные политики.

  По умолчанию параметр выключен.

В разделе **Расписание соединений** можно задать временные интервалы, в которые Агент администрирования будет передавать данные на Сервер администрирования:

- **Подключаться при необходимости**

  Если выбран этот вариант, подключение будет устанавливаться тогда, когда Агенту администрирования нужно передать данные на Сервер администрирования.

  По умолчанию выбран этот вариант.

- **Подключаться в указанные периоды**

  Если выбран этот вариант, подключение Агента администрирования к Серверу администрирования выполняется в заданные периоды времени. Можно добавить несколько периодов подключения.

Опрос сети точками распространения

В разделе **Опрос сети точками распространения** вы можете настроить автоматический опрос сети. Вы можете использовать следующие параметры, чтобы включить опрос и настроить его расписание:

- **Zeroconf**

  Если этот параметр включен, точка распространения автоматически опрашивает сеть с устройствами IPv6, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае включенный опрос IP-диапазонов игнорируется, так как точка распространения опрашивает всю сеть.

  Чтобы можно было начать использовать Zeroconf, должны быть выполнены следующие условия:

  - Точка распространения должна работать под управлением Linux.
  - Вам нужно установить утилиту avahi-browse на точку распространения.

  Если этот параметр отключен, точка распространения не опрашивает сети с устройствами IPv6.

  По умолчанию параметр выключен.

- **IP-диапазоны**

  Если этот параметр включен, точка распространения автоматически опрашивает IP-диапазоны в соответствии с расписанием, настроенным по кнопке **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.

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**

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".

История ревизий

На этой закладке вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат.

Задачи

В этом разделе описаны задачи, которые используются в Kaspersky Security Center.

О задачах

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

Вы можете создать задачу для программы в Kaspersky Security Center 14 Web Console, только если для этой программы установлен плагин управления на сервере Kaspersky Security Center 14 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 14 Web Console, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

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

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

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

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

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

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

Результаты выполнения задач сохраняются в журнале событий операционной системы на каждом устройстве, в журнале событий на Сервере администрирования и в базе данных Сервера администрирования.

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

Область задачи

Область задачи – 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.

Создание задачи

Чтобы создать задачу:

1. В главном окне программы перейдите в раздел **Устройства → Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте шагам мастера.

3. 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.
4. Нажмите на кнопку **Готово**.

Задача будет создана и отобразится в списке задач.

Чтобы создать задачу, назначенную выбранным устройствам:

1. В главном окне программы перейдите в раздел **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 **Создание задачи**.

   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.

Запуск задачи вручную

Программа 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 программы перейдите в раздел **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 выполнения**.

Просмотр списка задач

Вы можете просмотреть список задач, созданных в Kaspersky Security Center Linux.

Чтобы просмотреть список задач,

Перейдите в раздел **Устройства → Задачи**.

Отобразится список задач. Задачи сгруппированы по названиям программ, к которыми они относятся. Например, задача *Удаленная установка программы* относится к Серверу администрирования, а задача *Обновление* относится к Kaspersky Endpoint Security для Linux.

Чтобы просмотреть свойства задачи,

нажмите на имя задачи.

Окно свойств задачи отображается с несколькими именными закладками. Например, **Тип задачи** отображается на закладке **Общие**, а расписание задачи на закладке **Расписание**.

Общие параметры задач

Развернуть все | Свернуть все

Этот раздел содержит описание параметров, которые вы можете просмотреть и настроить для большинства ваших задач. Список доступных параметров зависит от настраиваемой задачи.

Параметры, заданные при создании задачи

Вы можете задать некоторые параметры при создании задачи. Некоторые из этих параметров можно также изменить в свойствах созданной задачи.

- Параметры перезагрузки операционной системы:
  - **Не перезагружать устройство**

    Клиентские устройства не будут автоматически перезагружаться после выполнения операции. Для завершения операции потребуется перезагрузить устройство (например, вручную или с помощью задачи управления устройствами). Информация о необходимости перезагрузки сохранена в результатах выполнения задачи и в статусе устройства. Этот вариант подходит для задач на серверах и других устройствах, для которых критически важна бесперебойная работа.

  - **Перезагрузить устройство**

В этом случае перезагрузка всегда выполняется автоматически, если перезагрузка требуется для завершения операции. Этот вариант подходит для задач на устройствах, для которых допустимы периодические перерывы в работе (выключение, перезагрузка).

- Принудительно закрывать программы в заблокированных сеансах

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

  Если этот параметр включен, такие программы на заблокированных устройствах принудительно закрываются перед перезагрузкой устройства. В результате пользователи могут потерять несохраненную работу.

  Если этот параметр выключен, заблокированное устройство не перезагружается. Состояние задачи на этом устройстве указывает на необходимость перезапуска устройства. Пользователям необходимо вручную закрыть все программы, которые запущены на заблокированных устройствах, и перезагрузить эти устройства.

  По умолчанию параметр выключен.

- Параметры расписания задачи:
  - **Параметры Запуск по расписанию:**
    - Каждый N час

      Задача выполняется регулярно, с заданным интервалом в часах, начиная с указанных даты и времени.

      По умолчанию задача запускается каждые 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 программой, для которой вы создаете задачу.

      По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

    - Каждую N неделю

      Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

      По умолчанию задача запускается 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 поддерживается 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 Linux.

      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. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. 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 задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- Окно Выбор устройств, которым будет назначена задача:

  - **Выбрать устройства, обнаруженные в сети Сервером администрирования**

В этом случае задача назначается набору устройств. В набор устройств вы можете включать как устройства в группах администрирования, так и нераспределенные устройства.

Например, вы можете использовать этот параметр в задаче установки Агента администрирования на нераспределенные устройства.

- **Задать адреса устройств вручную или импортировать из списка**

  Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

  Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

- **Назначить задачу выборке устройств**

  Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

  Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

- **Назначить задачу группе администрирования**

  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.

  Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

- Параметры учетной записи:

  - **Учетная запись по умолчанию**

    Задача будет запускаться под той же учетной записью, под которой была установлена и запущена программа, выполняющая эту задачу.

    По умолчанию выбран этот вариант.

  - **Задать учетную запись**

    В полях **Учетная запись** и **Пароль** укажите данные учетной записи, под которой должна запускаться задача. Учетная запись должна иметь необходимые права для выполнения задачи.

  - **Учетная запись**

    Учетная запись, от имени которой будет запускаться задача.

  - **Пароль**

    Пароль учетной записи, от имени которой будет запускаться задача.

Параметры, заданные после создания задачи

Вы можете задать следующие параметры только после создания задачи.

- Параметры групповой задачи:

  - **Распределить по подгруппам**

    Этот параметр доступен только в свойствах групповых задач.

    Когда этот параметр включен, область действия задачи включает в себя:

    - группу администрирования, которую вы выбрали при создании задачи;

- группы администрирования, подчиненные по отношению к выбранной группе администрирования на любом уровне вниз по иерархии групп.

Если этот параметр выключен, в состав задачи входит только та группа администрирования, которую выбрали при создании задачи.

По умолчанию параметр включен.

- Распространять на подчиненные и виртуальные Серверы администрирования

При включении этого параметра задача, действующая на главном Сервере администрирования, применяется и на подчиненных Серверах администрирования (в том числе виртуальных). Если на подчиненном Сервере администрирования уже существует задача такого же типа, то на подчиненном Сервере администрирования применяются обе задачи — существующая и унаследованная от главного Сервера администрирования.

Этот параметр доступен, только если параметр **Распределить по подгруппам** включен.

По умолчанию параметр выключен.

- Дополнительные параметры расписания:

  - Активировать устройство перед запуском задачи функцией Wake-on-LAN за (мин)

Если флажок установлен, операционная система на устройстве будет загружаться за указанное время до начала выполнения задачи. Время, заданное по умолчанию, – 5 минут.

Включите этот параметр, если вы хотите, чтобы задача выполнялась на всех клиентских устройствах из области задач, включая те устройства, которые выключены, когда задача вот-вот начнется.

Если нужно, чтобы устройства автоматически выключались после выполнения задачи, включите параметр **Выключать устройства после выполнения задачи**. Параметр находится в этом же окне.

По умолчанию параметр выключен.

  - Выключить устройство после завершения 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 задачу, если она выполняется более чем (мин)

По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

- Параметры уведомления:

  - Блок **Сохранять информацию о результатах**:

    - Хранить в базе данных Сервера администрирования в течение (сут)

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся на Сервере администрирования в течение указанного количества дней. По истечении этого периода информация удаляется с Сервера администрирования.

По умолчанию параметр включен.

    - Хранить в журнале событий ОС на устройстве

События программы, связанные с выполнением задачи, хранятся локально в системном журнале событий каждого клиентского устройства.

По умолчанию параметр выключен.

    - Хранить в журнале событий ОС на Сервере администрирования

События программы, связанные с выполнением задачи на всех клиентских устройствах из области задачи, хранятся централизованно в системном журнале событий операционной системы Сервера администрирования.

По умолчанию параметр выключен.

- **Сохранять все события**

  Если выбран этот параметр, в журнал событий записываются все события, связанные с задачей.

- **Сохранять события, связанные с ходом выполнения задачи**

  Если выбран этот параметр, в журнал событий записываются только события, связанные с выполнением задачи.

- **Сохранять только результат выполнения задачи**

  Если выбран этот параметр, в журнал событий записываются только события, связанные с результатами выполнения задачи.

- **Уведомлять администратора о результатах**

  Вы можете выбрать способы, с помощью которых администраторы получают уведомления о результатах выполнения задачи: по электронной почте, по SMS и при запуске исполняемого файла. Чтобы настроить параметры уведомления, перейдите по ссылке **Параметры**.

  По умолчанию отключены все способы уведомлений.

- **Уведомлять только об ошибках**

  Если этот параметр включен, администраторы получают уведомление, только если задача завершается с ошибкой.

  Если этот параметр выключен, администраторы получают уведомление после каждого завершения задачи.

  По умолчанию параметр включен.

- Параметры безопасности.
- Параметры области действия задачи.

  В зависимости от того, как определяется область действия задачи, присутствуют следующие параметры:

  - **Устройства**

    Если область действия задачи определяется группами администрирования, вы можете просмотреть эту группу. Никакие изменения здесь недоступны. Однако вы можете настроить **Исключения из области действия задачи**.

    Если область действия задачи определяется списком устройств, вы можете изменить этот список, добавив и удалив устройства.

  - **Выборка устройств**

    Вы можете изменить выборку устройств, к которым применяется задача.

  - **Исключения из области действия задачи**

    Вы можете указать группу устройств, к которым не применяется задача. Группы, подлежащие исключению, могут быть только подгруппами группы администрирования, к которой применяется задача.

- **История ревизий**.

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. На закладке **Устройства** выберите **Задачи**.
2. Нажмите на кнопку **Управление учетными данными учетной записи для запуска задач**.

Следуйте далее указаниям мастера.

Шаг 1. Выбор учетных данных

Развернуть все | Свернуть все

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 14 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.

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.

Шаг 3. Просмотр результатов

На последнем шаге мастера просмотрите результаты для каждой из обнаруженных задач. Для завершения работы мастера нажмите на кнопку **Готово**.

Просмотр результатов выполнения задач, хранящихся на Сервере администрирования

Kaspersky Security Center Linux 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**.

Управление клиентскими устройствами

Kaspersky Security Center Linux позволяет управлять клиентскими устройствами:

- Просматривать параметры и статусы управляемых устройств, в том числе кластеров и массивов серверов.
- Настраивать точки распространения.
- Управлять задачами.

Группы администрирования можно использовать для объединения клиентских устройств в набор, которым можно управлять как единым целым. Клиентское устройство может быть включено только в одну группу администрирования. Устройства могут быть автоматически отнесены к группе на основе **Условия правила**:

- Создание правил перемещения устройств.
- Копирование правил перемещения устройств.
- Условия для правила перемещения устройств.

Вы можете использовать выборки устройств, чтобы для фильтровать устройства по условию. Вы также можете назначать теги устройствам для создания выборок устройств, поиска устройств и распределения устройств между группами администрирования.

Параметры управляемого устройства

Развернуть все | Свернуть все

Чтобы просмотреть параметры управляемого устройства:

1. Выберите **Устройства** → **Управляемые устройства**.

   Отобразится список управляемых устройств.

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

Откроется окно свойств выбранного устройства.

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

- **Общие**

  Эта вкладка содержит следующие разделы:

  - Раздел **Общие** содержит общую информацию о клиентском устройстве. Информация предоставляется на основании данных, полученных в ходе последней синхронизации клиентского устройства с Сервером администрирования:
    - **Имя**

      В поле можно просмотреть и изменить имя клиентского устройства в группе администрирования.

    - **Описание**

      В поле можно ввести дополнительное описание клиентского устройства.

    - **Полное название группы**

      Группа администрирования, в состав которой входит клиентское устройство.

    - **Последнее обновление защиты**

      Дата последнего обновления антивирусных баз или программ на устройстве.

    - **Последнее появление в сети**

      Дата и время, когда устройство последний раз было видимо в сети.

- **Соединение с Сервером администрирования**

  Дата и время последнего соединения Агента администрирования, установленного на клиентском устройстве, с Сервером администрирования.

- **Не разрывать соединение с Сервером администрирования**

  Если этот параметр включен, сохраняется постоянное соединение между управляемым устройством и Сервером администрирования. Вы можете использовать этот параметр, если не используете push-серверы, которые обеспечивают такое соединение.

  Если параметр выключен и push-серверы не используются, управляемое устройство подключается к Серверу администрирования для синхронизации данных или передачи информации.

  Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

  Этот параметр по умолчанию выключен на управляемых устройствах. Этот параметр включен по умолчанию на устройстве, на котором установлен Сервер администрирования, и остается включенным, даже если вы попытаетесь его выключить.

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

  - **IP-адрес**

    IP-адрес устройства.

  - **Windows-домен**

    Рабочая группа, содержащая устройство.

  - **DNS-имя**

    Имя DNS-домена клиентского устройства.

  - **NetBIOS-имя**

    NetBIOS-имя клиентского устройства.

- В разделе **Система** представлена информация об операционной системе, установленной на клиентском устройстве.

- В разделе **Защита** представлена следующая информация о состоянии антивирусной защиты на клиентском устройстве:

  - **Статус устройства**

    Статус клиентского устройства, формируемый на основании установленных администратором критериев состояния антивирусной защиты на устройстве и активности устройства в сети.

  - **Все проблемы**

    Эта таблица содержит полный список проблем, обнаруженных управляемыми программами, установленными на клиентском устройстве. Каждая проблема имеет статус, который управляемая программа предлагает вам назначить устройству из-за этой проблемы.

  - **Постоянная защита**

    Статус текущего состояния постоянной защиты клиентского устройства.

    После того как статус изменяется на устройстве, новый статус отображается в окне свойств устройства только после синхронизации клиентского устройства с Сервером администрирования.

  - **Последняя проверка по требованию**

    Дата и время последнего поиска вредоносного ПО на клиентском устройстве.

- Всего обнаружено угроз

  Общее количество обнаруженных на клиентском устройстве угроз с момента установки программы безопасности (первой проверки устройства) либо с момента последнего обнуления счетчика угроз.

- Активные угрозы

  Количество необработанных файлов на клиентском устройстве.

  В поле не учитывается количество необработанных файлов для мобильных устройств.

- В разделе **Статус устройства определен программой** отображается информация о статусе устройства, который определен управляемой программой, установленной на клиентском устройстве. Это состояние устройства может отличаться от того, которое определено Kaspersky Security Center Linux.

- Программы

  На этой вкладке отображается список программ "Лаборатории Касперского", установленных на клиентском устройстве. На этой вкладке находятся кнопки **Запустить** и **Остановить**, которые позволяют запускать и останавливать выбранную программу "Лаборатории Касперского" (кроме Агента администрирования). Вы можете использовать эти кнопки, если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования. Если управляемое устройство недоступно для push-уведомлений, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** в разделе **Общие** включен), кнопки **Запустить** и **Остановить** активны. Иначе при попытке запустить или остановить программу появится сообщение об ошибке. Также вы можете нажать на имя программы, чтобы просмотреть общую информацию о программе, список событий, произошедших на устройстве, и параметры программы.

- Действующие политики и профили политик

  На этой закладке отображаются списки политик и профилей политик, которые назначены управляемому устройству.

- Задачи

  На закладке **Задачи** вы можете управлять задачами клиентского устройства: просматривать список существующих задач, создавать новые, удалять, запускать и останавливать задачи, изменять их параметры и просматривать результаты выполнения. Список задач предоставляется на основании данных, полученных в ходе последней синхронизации клиента с Сервером администрирования. Информация о статусе задач запрашивается Сервером администрирования с клиентского устройства. Если на управляемых устройствах доступен порт 15000 UDP для приема запросов на связь с Сервером администрирования, отображается статус задачи и кнопки управления задачей активны. Если управляемое устройство недоступно для push-уведомлений, но включен режим постоянного подключения к Серверу администрирования (параметр **Не разрывать соединение с Сервером администрирования** в разделе **Общие** включен), действия с задачами доступны.

  В случае отсутствия связи статус не отображается и кнопки неактивны.

- События

  На закладке **События** отображаются события, зарегистрированные на Сервере администрирования для выбранного клиентского устройства.

- Теги

  На закладке **Теги** можно управлять списком ключевых слов, на основании которых выполняется поиск клиентского устройства: просматривать список существующих тегов, назначать теги из списка, настраивать правила автоматического назначения тегов, добавлять новые теги и переименовывать старые теги, удалять теги.

- Дополнительно

  Эта вкладка содержит следующие разделы:

  - **Реестр программ**. В этом разделе можно просмотреть реестр установленных на клиентском устройстве программ и обновлений для них, а также настроить отображение реестра программ.

    Информация об установленных программах предоставляется в том случае, если установленный на клиентском устройстве Агент администрирования передает необходимую информацию на Сервер администрирования. Параметры передачи информации на Сервер администрирования можно настроить в окне свойств Агента администрирования или его политики в разделе **Хранилища**.

    При нажатии на имя программы открывается окно, содержащее сведения о программе и список пакетов обновлений, установленных для этой программы.

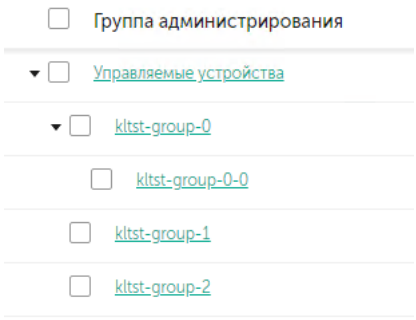
- **Исполняемые файлы**. В этом разделе отображаются исполняемые файлы, обнаруженные на клиентском устройстве.
- **Точки распространения**. В этом разделе представлен список точек распространения, с которыми взаимодействует устройство.
  - Экспортировать в файл

    По кнопке **Экспортировать в файл** вы можете сохранить в файл список точек распространения, с которыми взаимодействует устройство. По умолчанию программа экспортирует список устройств в файл формата CSV.
  - Свойства

    По кнопке **Свойства** вы можете посмотреть и настроить параметры точки распространения, с которым взаимодействует устройство.
- **Реестр оборудования**. В этом разделе можно просмотреть информацию об оборудовании, установленном на клиентском устройстве.

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).



Просмотр иерархии групп администрирования

Чтобы создать группу администрирования:

1. Перейдите в раздел **Устройства** → **Иерархия групп**.
2. В структуре группы администрирования выберите группу администрирования, в состав которой должна входить новая группа администрирования.
3. Нажмите на кнопку **Добавить**.
4. В открывшемся окне **Имя новой группы администрирования** введите имя группы и нажмите на кнопку **Добавить**.

В результате в иерархии групп администрирования появится новая группа администрирования с заданным именем.

Чтобы создать структуру групп администрирования:

1. Перейдите в раздел **Устройства** → **Иерархия групп**.
2. Нажмите на кнопку **Импортировать**.

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. 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 Linux в явном виде, в разделе **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 снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

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 программ* 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 Linux (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

Создание правил перемещения устройств

Развернуть все | Свернуть все

Можно настроить правила перемещения устройств, в соответствии с которыми устройства будут распределены по группам администрирования.

Чтобы создать правило перемещения устройств:

1. В главном окне программы перейдите в раздел **Устройства → Правила перемещения**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне укажите следующие данные на закладке **Общие**:

- **Имя правила**

  Укажите имя нового правила активации.

  Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

- **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

  Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

- **Применять правило постоянно**

  Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Включить правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

4. На закладке **Условия правила** укажите хотя бы один критерий, по которому устройства будут перемещены в группу администрирования.
5. Нажмите на кнопку **Сохранить**.

Будет создано правило перемещения. Оно появится в списке правил перемещения.

Чем выше положение правила в списке, тем выше его приоритет. Чтобы повысить или понизить приоритет правила перемещения, с помощью мыши переместите правило вверх или вниз по списку соответственно.

Если 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).

Копирование правил перемещения устройств

Развернуть все | Свернуть все

Можно копировать правила перемещения устройств, например, если требуется несколько одинаковых правил для разных целевых групп администрирования.

Чтобы скопировать правило перемещения устройств:

1. Выполните одно из следующих действий:
   - В главном окне программы перейдите в раздел **Устройства → Правила перемещения**.
   - В главном окне программы перейдите в раздел **Обнаружение устройств и развертывание → Развертывание и назначение → Правила перемещения**.

   Отобразится список правил перемещения устройств.
2. Установите флажок напротив правила, которое требуется скопировать.
3. Нажмите на кнопку **Копировать**.
4. В открывшемся окне при необходимости измените данные на закладке **Общие** либо оставьте существующие значения, если требуется только скопировать правило, без изменения параметров:
   - **Имя правила**

     Укажите имя нового правила активации.

Если вы копируете правило, новое правило получает такое же имя, как и исходное правило, но к нему добавляется индекс в скобках, например: (1).

- **Группа администрирования**

  Выберите группу администрирования, в которую будут автоматически перемещаться устройства.

- **Применить правило**

  Вы можете выбрать один из следующих вариантов:

  - **Выполнять один раз для каждого устройства**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям.

  - **Выполнять один раз для каждого устройства и при каждой установке Агента администрирования**

    Правило применяется однократно для каждого устройства, соответствующего указанным критериям, а затем только при переустановке Агента администрирования на этих устройствах.

  - **Применять правило постоянно**

    Правило применяется в соответствии с расписанием, автоматически задаваемым на Сервере администрирования (обычно каждые несколько часов).

- **Перемещать только устройства, которые не входят ни в одну группу администрирования**

  Если этот параметр включен, только нераспределенные устройства будут перемещены в выбранную группу.

  Если этот параметр выключен, устройства, которые уже принадлежат другим группам администрирования, а также нераспределенные устройства, будут перемещены в выбранную группу.

- **Включить правило**

  Если этот параметр включен, правило включено и начинает применяться сразу после сохранения.

  Если этот параметр выключен, правило создается, но оно не включено. Правило не будет работать до тех пор, пока вы не включите этот параметр.

5. На закладке **Условия правила** укажите критерии для устройств, которые требуется переместить автоматически.
6. Нажмите на кнопку **Сохранить**.

Будет создано новое правило перемещения. Оно появится в списке правил перемещения.

Условия для правила перемещения устройств

Развернуть все | Свернуть все

При создании или копировании правила перемещения клиентских устройств в группы администрирования на вкладке **Условия правила** вы задаете условия перемещения устройств. Чтобы определить, какие устройства следует перемещать, можно использовать следующие критерии:

- Теги, присвоенные клиентским устройствам.
- Параметры сети. Например, вы можете перемещать устройства с IP-адресами из указанного диапазона.
- Управляемые программы, установленные на клиентских устройствах, например Агент администрирования или Сервер администрирования.
- Виртуальные машины, которые являются клиентскими устройствами.

Ниже вы можете найти описание того, как указать эту информацию в правиле перемещения устройств.

Если в правиле указано несколько условий, срабатывает логический оператор AND и применяются все условия одновременно. Если вы не выберете какие-либо параметры или оставите некоторые поля пустыми, такие условия не применяются.

Закладка Теги

На этой закладке можно настроить поиск устройств по ключевым словам (тегам), которые были добавлены ранее в описания клиентских устройств. Для этого выберите необходимые теги. Кроме того, вы можете включить следующие параметры:

- **Применить к устройствам без выбранных тегов**

Если этот параметр включен, все устройства с указанными тегами исключаются из правила перемещения устройств. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

По умолчанию параметр выключен.

- **Применить, если есть хотя бы один из выбранных тегов**

  Если этот параметр включен, правило перемещения устройств применяется к клиентским устройствам хотя бы с одним из выбранных тегов. Если этот параметр выключен, правило перемещения устройств применяется к устройствам со всеми выбранными тегами.

  По умолчанию параметр выключен.

Закладка Сеть

На этой закладке вы можете указать сетевые данные устройств, которые учитывает правило перемещения устройств:

- **DNS-имя устройства**

  DNS-имя домена клиентского устройства, которое вы хотите переместить. Заполните это поле, если в вашей сети есть DNS-сервер.

  Если для базы данных, которую вы используете для Kaspersky Security Center, настроена сортировка с учетом регистра, учитывайте регистр при указании DNS-имени устройства. Иначе правило перемещения устройств не будет работать.

- **DNS-домен**

  Правило перемещения устройств применяется ко всем устройствам, включенным в указанный основной DNS-суффикс. Заполните это поле, если в вашей сети есть DNS-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.

- **IP-адрес подключения к Серверу администрирования**

  Если этот параметр включен, можно задать IP-адреса, по которым клиентские устройства подключаются к Серверу администрирования. Для этого укажите IP-диапазон, включающий все необходимые IP-адреса.

  По умолчанию параметр выключен.

- **Изменение профиля подключения**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам с измененным профилем подключения.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, профиль подключения которых не изменялся.
  - **Значение не выбрано**. Условие не применяется.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

Закладка Программы

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

- **Агент администрирования установлен**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, на которых установлен Агент администрирования.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, на которых не установлен Агент администрирования.
  - **Значение не выбрано**. Условие не применяется.

- **Программы**

  Укажите, какие управляемые программы должны быть установлены на клиентских устройствах, чтобы к этим устройствам применялось правило перемещения устройств. Например, вы можете выбрать **Агент администрирования Kaspersky Security Center 14** или **Сервер администрирования Kaspersky Security Center 14**.

  Если вы не выберете управляемую программу, условие не будет применяться.

- **Версия операционной системы**

  Можно выбирать клиентские устройства на основе версии операционной системы. Для этого укажите операционные системы, которые должны быть установлены на клиентских устройствах. В результате правило перемещения устройств применяется к клиентским устройствам с выбранными операционными системами.

  Если этот параметр выключен, условие не применяется. По умолчанию параметр выключен.

- **Архитектура операционной системы**

  Можно выбирать клиентские устройства по разрядности операционной системы. В поле **Архитектура операционной системы** можно выбрать одно из следующих значений:

  - **Нет данных**
  - **x86**
  - **AMD64**
  - **IA64**

  Чтобы проверить разрядность операционной системы клиентских устройств:

  1. В главном окне программы перейдите в раздел **Устройства** → **Управляемые устройства**.
  2. Нажмите на кнопку **Параметры столбцов** справа ( ).
  3. Выберите параметр **Архитектура операционной системы** и нажмите на кнопку **Сохранить**.

     После этого для каждого управляемого устройства отобразится разрядность операционной системы.

- **Версия пакета обновления операционной системы**

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- **Пользовательский сертификат**

  Выберите одно из следующих значений:

  - **Установлено**. Правило перемещения устройств применяется только к мобильным устройствам с мобильным сертификатом.
  - **Не установлена**. Правило перемещения устройств применяется только к мобильным устройствам без мобильного сертификата.
  - **Значение не выбрано**. Условие не применяется.

- Номер сборки операционной системы

  Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

- Номер выпуска операционной системы

  Этот параметр применим только для операционных систем Windows.

  Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить правило перемещения устройств для всех номеров сборки, кроме указанного.

Закладка Виртуальные машины

На этой закладке 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

  В раскрывающемся списке можно выбрать одно из следующих значений:
  - **Неизвестно**. Условие не применяется.
  - **Нет**. Перемещаемые устройства не должны являться виртуальными машинами.
  - **Да**. Перемещаемые устройства должны являться виртуальными машинами.

- **Тип виртуальной машины**

- Часть Virtual Desktop Infrastructure

  В раскрывающемся списке можно выбрать одно из следующих значений:
  - **Неизвестно**. Условие не применяется.
  - **Нет**. Перемещаемые устройства не должны являться частью VDI.
  - **Да**. Перемещаемые устройства должны являться частью VDI.

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. Перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Перейдите по ссылке **Текущий путь**: `<current path>` над списком.
3. В открывшемся окне выберите группу администрирования, в которую требуется добавить устройства.
4. Нажмите на кнопку **Добавить устройства**.

   В результате запустится мастер перемещения устройств.
5. Составьте список устройств, которые вы хотите добавить в группу администрирования.

В список устройств могут быть добавлены только те устройства, информация о которых уже была добавлена в базу данных Сервера администрирования при подключении устройства или в результате обнаружения устройств.

Выберите, как вы хотите добавить устройства в список:

- Нажмите на кнопку **Добавить устройства** и укажите устройства одним из следующих способов:
  - Выберите устройства из списка устройств, обнаруженных Сервером администрирования.
  - Укажите IP-адреса устройств или IP-диапазон.
  - Укажите 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.

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. 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 **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.

Смена Сервера администрирования для клиентских устройств

Развернуть все | Свернуть все

Вы можете сменить Сервер администрирования на другой для конкретных клиентских устройств. Для этого используйте задачу *Смена Сервера администрирования*.

Чтобы сменить Сервер администрирования, под управлением которого находятся клиентские устройства, другим Сервером:

1. Подключитесь к Серверу администрирования, под управлением которого находятся устройства.
2. Создайте задачу обслуживания Сервера администрирования.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера. В окне мастера добавления задач **Новая задача** выберите программу **Kaspersky Security Center 14** и тип задачи **Смена Сервера 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.

     Если задача назначена группе администрирования, вкладка **Безопасность** не отображается в окне свойств задачи, так как групповые задачи подчиняются параметрам групп безопасности, к которым они относятся.

   - **Задать адреса устройств вручную или импортировать из списка**

     Вы можете задавать DNS-имена, IP-адреса, а также диапазоны IP-адресов устройств, которым нужно назначить задачу.

     Вы можете использовать этот параметр для выполнения задачи для заданной подсети. Например, вы можете установить определенную программу на устройства бухгалтеров или проверять устройства в подсети, которая, вероятно, заражена.

   - **Назначить задачу выборке устройств**

     Задача назначается устройствам, входящим в выборку устройств. Можно указать одну из существующих выборок.

     Например, вы можете использовать этот параметр, чтобы запустить задачу на устройствах с определенной версией операционной системы.

3. Запустите созданную задачу.

После завершения работы задачи клиентские устройства, для которых она была создана, переходят под управление Сервера администрирования, указанного в параметрах задачи.

Перемещение устройств, подключенных к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования

Вы можете перемещать устройства, подключенные к Серверу администрирования через шлюзы соединения, на другой Сервер администрирования Например, это может потребоваться, если вы устанавливаете другую версию Сервера администрирования и не хотите переустанавливать Агент администрирования на устройствах, поскольку это может занять много времени.

Команды, описанные в инструкции, нужно выполнить на клиентских устройствах под учетной записью с правами администратора.

Чтобы переместить устройство, подключенное через шлюз соединения, на другой Сервер администрирования:

1. Запустите утилиту klmover с параметром `-address <адрес Сервера>`, чтобы переключиться на новый Сервер администрирования.
2. Выполните команду `klnagchk -nagwait -tl 4`.
3. Выполните следующие команды для установки нового шлюза соединения:

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "gateway_ip_or_name" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Здесь `gateway_ip_or_name` – адрес шлюза соединения, доступного из интернета.

   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` – это номер TCP-порта, который прослушивает шлюз соединения.

4. Выполните команду `klnagchk -restart -tl 4` для запуска службы Агента администрирования.

Устройство будет перемещено на новый Сервер администрирования и подключено через новый шлюз соединения.

Просмотр и настройка действий, когда устройство неактивно

Развернуть все | Свернуть все

Если клиентские устройства группы администрирования неактивны, вы можете получать уведомления об этом. Вы также можете автоматически удалять такие устройства.

Чтобы просмотреть или настроить действия, когда устройства неактивны в группе администрирования:

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. Выберите имя требуемой группы администрирования.

   Откроется окно свойств группы администрирования.
3. В окне свойств перейдите на закладку **Параметры**.
4. В разделе **Наследование** включите или выключите следующие параметры:

   - **Наследовать из родительской группы**

     Если флажок установлен, параметры в этом разделе будут наследоваться из родительской группы, в которую входит клиентское устройство. Если флажок установлен, параметры в блоке параметров **Активность устройств в сети** недоступны для изменения.

     Этот параметр доступен только для группы администрирования, у которой есть родительская группа администрирования.

     По умолчанию параметр включен.

   - **Обеспечить принудительное наследование параметров для дочерних групп**

     Значения параметров будут распределены по дочерним группам, но в свойствах дочерних групп эти параметры недоступны для изменений.

     По умолчанию параметр выключен.
5. В разделе **Активность устройств** включите или выключите следующие параметры:

   - **Уведомлять администратора, если устройство неактивно больше (сут)**

     Если этот параметр включен, администратор получает уведомления о неактивности устройств. В поле ввода можно задать интервал времени, по истечении которого будет сформировано событие **Устройство долго не проявляет активности в сети**. Временной интервал, установленный по умолчанию, составляет 7 дней.

     По умолчанию параметр включен.

   - **Удалять устройство из группы, если оно неактивно больше (сут)**

     Если этот параметр включен, вы можете указать временной интервал, после которого устройство автоматически удаляется из группы администрирования. Временной интервал, установленный по умолчанию, составляет 60 дней.

     По умолчанию параметр включен.
6. Нажмите на кнопку **Сохранить**.

Ваши изменения сохранены и применены.

О статусах устройства

Kaspersky Security Center Linux 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 Linux учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center Linux 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.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Программа безопасности не установлена	Агент администрирования установлен на устройстве, но не установлена программа безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено 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.
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 вирусов	Устройство видимо в сети и на устройстве установлена программа безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые программы	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Есть необработанные инциденты	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен. • Переключатель включен.
Статус устройства определен программой	Статус устройства определяется управляемой программой.	• Переключатель выключен. • Переключатель включен.

На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, 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 программа безопасности на устройстве отключена больше указанного времени. В этом случае состояние программы безопасности *Остановлена* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Программа безопасности не запущена	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Переключатель выключен. • Переключатель включен.

Kaspersky Security Center Linux 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 *OK*.

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 Linux с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center Linux присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите закладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический", если** включите условие, чтобы переключить устройство в состояние *Критическое*.

   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 **OK**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне программы перейдите в раздел **Устройства → Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите закладку **Статус устройства**.
4. Выберите раздел **Предупреждение**.
5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   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*.

Политики и профили политик

В Kaspersky Security Center 14 Web Console можно создавать политики для программ "Лаборатории Касперского". В этом разделе описаны политики и профили политик, а также приведены инструкции по их созданию и изменению.

О политиках и профилях политик

Политика – это набор параметров программы "Лаборатории Касперского", которые применяются к группе администрирования и ее подгруппе. Вы можете установить несколько программ "Лаборатории Касперского" на устройства группы администрирования. Kaspersky Security Center предоставляет по одной политике для каждой программы "Лаборатории Касперского" в группе администрирования. Политика имеет один из следующих статусов:

Статус политики

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

Политики действуют по следующим правилам:

- Для одной программы можно настроить несколько политик с различными значениями.
- Для одной программы может быть активна только одна политика.
- Политика может иметь дочерние политики.

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

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

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

Профили политик работают по следующим правилам:

- Профиль политики вступает в силу при возникновении определенного условия активации.

- Профили политики содержат значения параметров, которые отличаются от параметров политики.
- Активация профиля политики изменяет эффективные параметры управляемого устройства.
- В политике может быть не более 100 профилей.

Блокировка (замок) и заблокированные параметры

У каждого параметра политики есть значок замка (). В таблице ниже показаны состояния значка замка:

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 управляемой программы. 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 управляемой программы. Такие параметры называются *заблокированными*.

Рекомендуется заблокировать параметры политики, которые вы хотите применить к управляемым устройствам. Разблокированные параметры политики могут быть переназначены параметрами программы "Лаборатории Касперского" на управляемом устройстве.

Вы можете использовать значок замка для выполнения следующих действий:

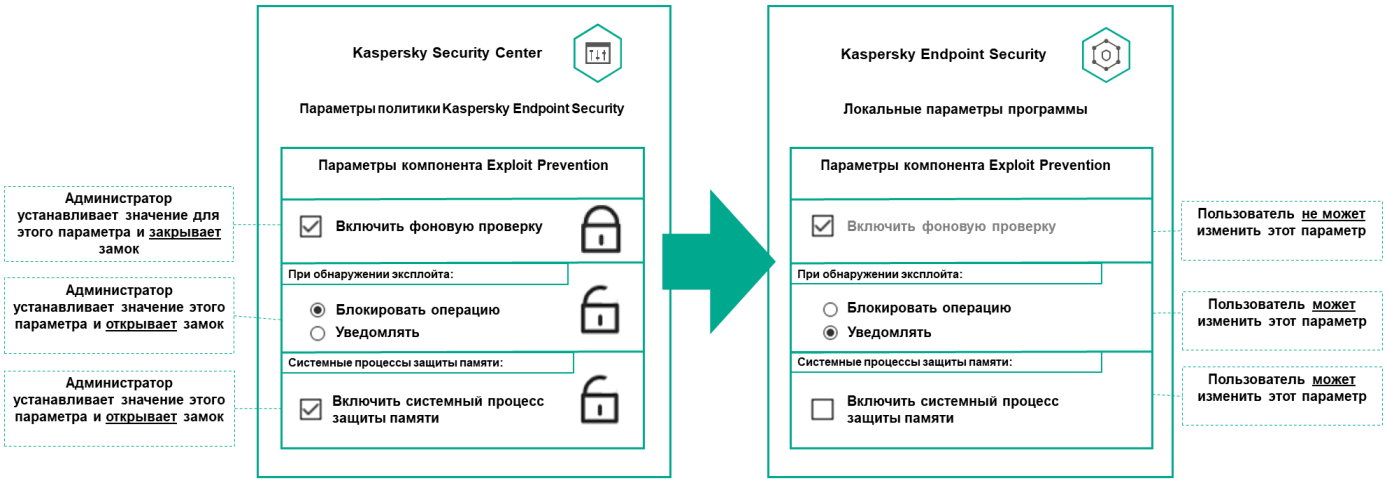
- Блокировка параметров для политики подгруппы администрирования.
- Блокировка параметров программы "Лаборатории Касперского" на управляемом устройстве.

Таким образом, заблокированный параметр используется в эффективных параметрах на управляемом устройстве.

Применение эффективных параметров включает в себя следующие действия:

- Управляемое устройство применяет значения параметров программы "Лаборатории Касперского".
- Управляемое устройство применяет заблокированные значения параметров политики.

Политика и управляемая программа "Лаборатории Касперского" содержат одинаковый набор параметров. При настройке параметров политики параметры программы "Лаборатории Касперского" меняют значения на управляемом устройстве. Вы не можете изменить заблокированные параметры на управляемом устройстве (см. рисунок ниже):



Замки и параметры программы "Лаборатории Касперского"

Наследование политик и профилей политик

В этом разделе представлена информация об иерархии и наследовании политик и профилей политик.

Иерархия политик

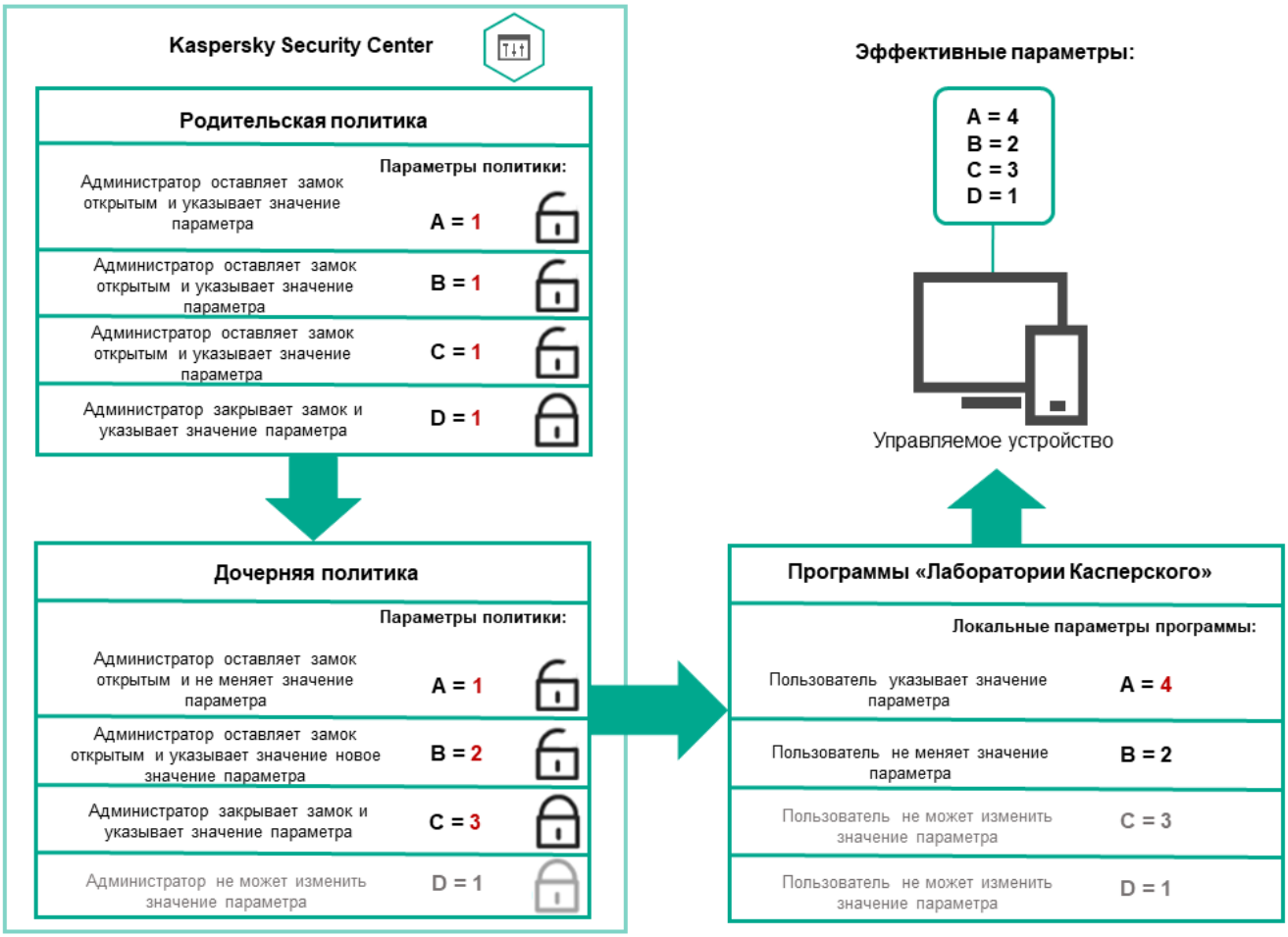
Если для разных устройств требуются разные параметры, вы можете объединить устройства в группы администрирования.

Вы можете указать политику для отдельной группы администрирования. Параметры политики можно *унаследовать*. Наследование – это получение значений параметров политики в подгруппах (дочерних группах) от вышестоящей политики (родительской) группы администрирования.

Политика, созданная для родительской группы, также называется *родительской политикой*. Политика, созданная для подгруппы (дочерней группы), также называется *дочерней политикой*.

По умолчанию на Сервере администрирования существует как минимум одна группа администрирования управляемых устройств. Если вы хотите создать группы администрирования, они создаются как подгруппы (дочерние группы) в группе Управляемые устройства.

Политики одной и той же программы действуют друг на друга по иерархии групп администрирования. Заблокированные параметры из политики вышестоящей (родительской) группы администрирования будут переназначать значения параметров политики подгруппы (см. рисунок ниже).

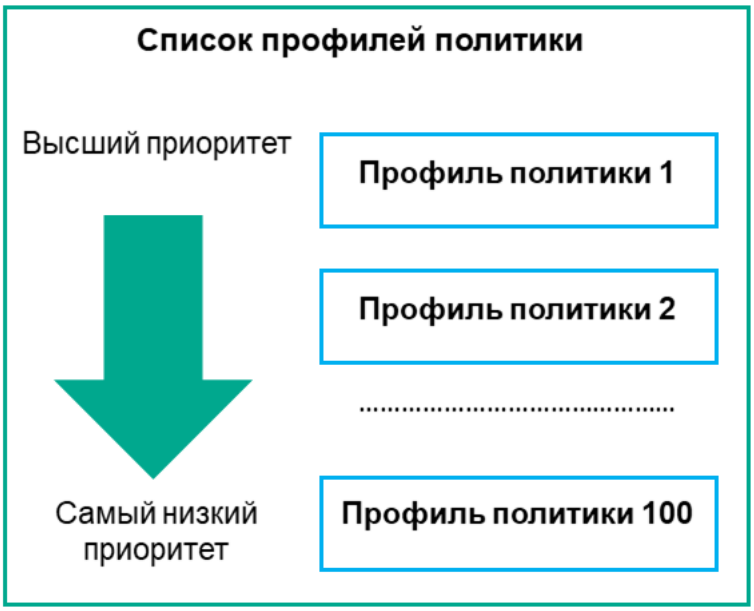


Иерархия политик

Профили политик в иерархии политик

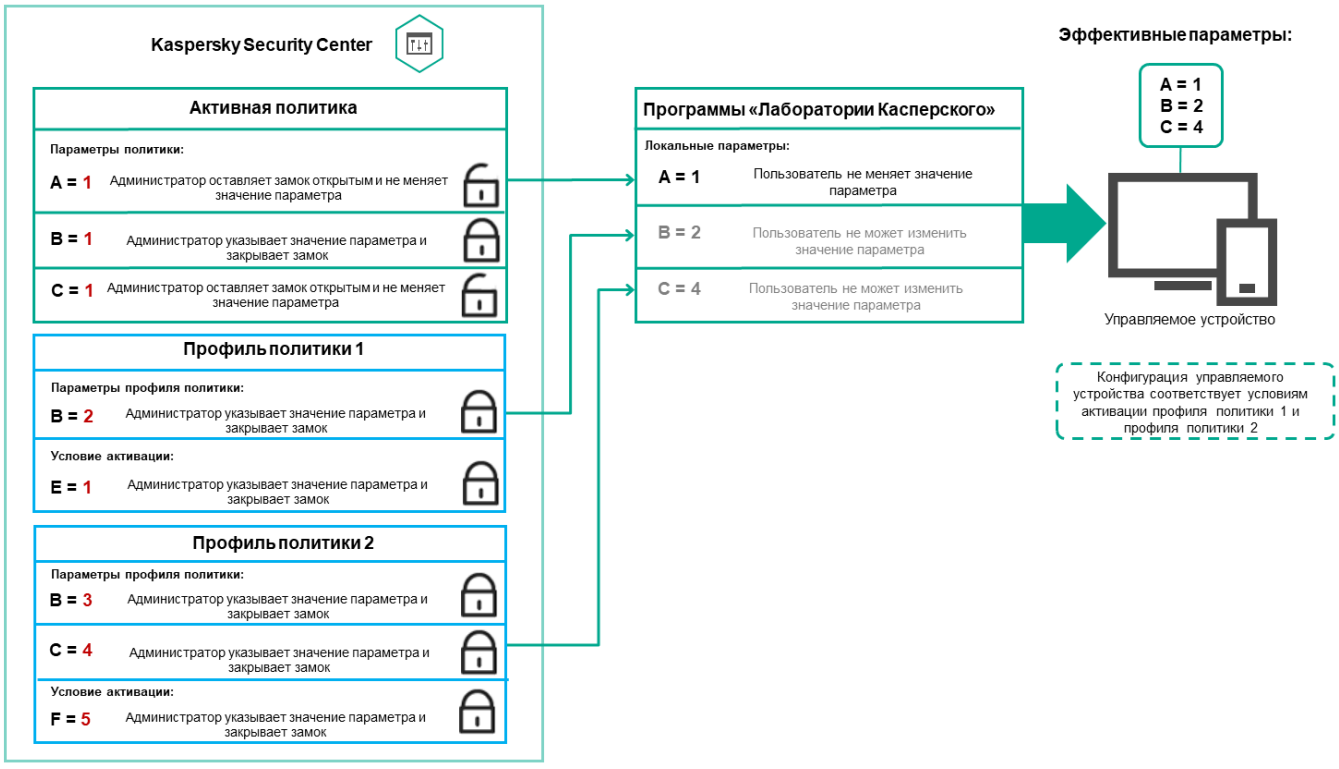
Профили политики имеют следующие условия назначения приоритета:

- 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).



Определение приоритета профиля политики

- 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).

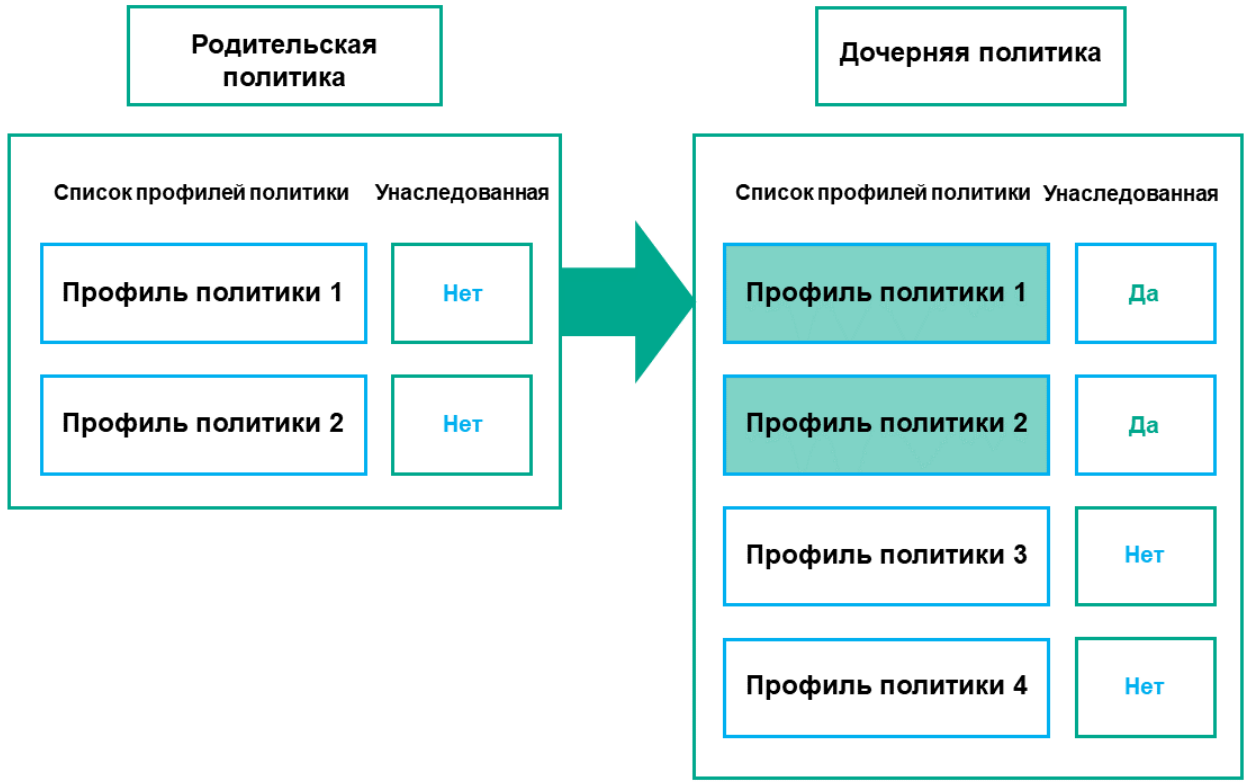


Конфигурация управляемого устройства соответствует условиям активации нескольких профилей политик

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).

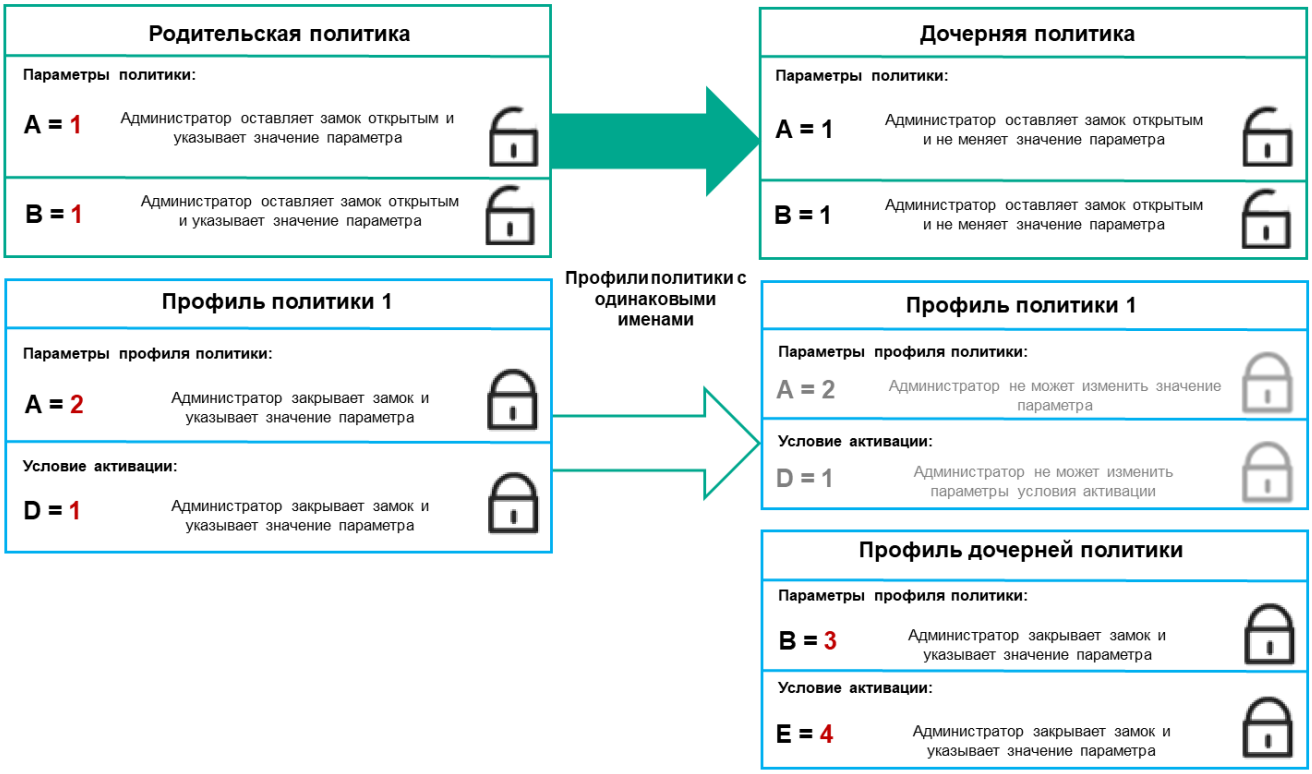


Наследование параметров профилей политики

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).



Дочерний профиль наследует значения параметров из родительского профиля политики

- 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.

Как реализуются параметры управляемого устройства

Применения эффективных параметров на управляемом устройстве можно описать следующим образом:

- Значения всех незаблокированных параметров берутся из политики.
- Затем они перезаписываются значениями параметров управляемой программы.
- Далее применяются заблокированные значения параметров из действующей политики. Значения заблокированных параметров изменяют значения разблокированных действующих параметров.

Управление политиками

В этом разделе описывается управление политиками и дается информация о просмотре списка политик, создании политики, изменении политики, копировании политики, перемещении политики, принудительной синхронизации, просмотре диаграммы состояния распространения политики и удалении политики.

Просмотр списка политик

Вы можете просмотреть список политик, созданных на Сервере администрирования или в любой группе администрирования.

Чтобы просмотреть список политик:

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В списке групп администрирования выберите группу администрирования, для которой вы хотите просмотреть список политик.

   Политики отобразятся в виде таблицы. Если политик нет, отобразится пустая таблица. Вы можете отображать или скрывать столбцы таблицы, изменять их порядок, просматривать только строки, которые содержат указанное вами значение, или использовать поиск.

Создание политики

Вы можете создавать политики; вы можете также изменять или удалять существующие политики.

Чтобы создать политику:

1. Перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите группу администрирования, для которой нужно создать политику:
   - Для корневой группы.

     В этом случае вы можете перейти к следующему шагу.
   - Для подгруппы:

     a. Нажмите на ссылку текущего пути в верхней части окна.

     b. В открывшейся панели нажмите на ссылку с названием нужной подгруппы.

     Текущий путь изменится в соответствии с выбранной подгруппой.
3. Нажмите на кнопку **Добавить**.

   Откроется окно **Выберите программу**.
4. Выберите программу, для которой требуется создать политику.
5. Нажмите на кнопку **Далее**.

   Откроется окно параметров новой политики на закладке **Общие**.
6. При желании вы можете изменить следующие параметры политики, заданные по умолчанию: имя, состояние и наследование.
7. Выберите закладку **Параметры программы**.

   Или нажмите на кнопку **Сохранить**, чтобы выйти. Политика появится в списке политик, и вы сможете изменить ее свойства позже.
8. В левой области закладки **Параметры программы** выберите нужный вам раздел и в панели результатов измените параметры политики. Вы можете изменить параметры политики в каждом разделе.

   Набор параметров зависит от программы, для которой вы создаете политику. Подробную информацию см. в следующих источниках:
   - Настройка Сервера администрирования

- Параметры политики Агента администрирования
- Онлайн-справка Kaspersky Endpoint Security для Linux

Подробнее о параметрах других программ безопасности см. в документации к соответствующей программе.

Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

9. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения политики.

В результате добавленная политика отображается в списке политик.

Общие параметры политик

Развернуть все | Свернуть все

Общие

На закладке **Общие** можно изменить состояние политики и настроить наследование параметров политики:

- В блоке **Состояние политики** можно выбрать один из вариантов действия политики:
  - **Активна**

    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.
  - **Неактивна**

    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 родительской политики**

    Если параметр включен, значения параметров политики наследуются из политики для группы верхнего уровня иерархии и недоступны для изменения.

    По умолчанию параметр включен.
  - **Обеспечить принудительное наследование параметров для дочерних политик**

    Если параметр включен, после применения изменений в политике будут выполнены следующие действия:
    - значения параметров политики будут распространены на политики вложенных групп администрирования – дочерние политики;
    - в блоке **Наследование параметров** раздела **Общие** окна свойств каждой дочерней политики будет автоматически включен параметр **Наследовать параметры родительской политики**.

    Когда параметр включен, значения параметров дочерних политик недоступны для изменения.

    По умолчанию параметр выключен.

Настройка событий

На закладке **Настройка событий** можно настроить регистрацию событий и оповещение о событиях. События распределены по уровням важности на закладках:

- **Критическое**

  Раздел **Критическое** 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 закладке свойств Сервера администрирования (например, адрес получателя). Если вы хотите, измените эти параметры на закладках **Электронная почта**, **SMS** и **Исполняемый файл для запуска**.

История ревизий

На закладке **История ревизий** вы можете просмотреть список ревизий политики и изменения, для которых был выполнен откат.

Изменение политики

Чтобы изменить политику:

1. Перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Выберите политику, которую требуется изменить.

   Откроется окно свойств политики.
3. Укажите общие параметры и параметры программы, для которой вы создаете политику. Подробную информацию см. в следующих источниках:

   - Настройка Сервера администрирования
   - Параметры политики Агента администрирования
   - Онлайн-справка Kaspersky Endpoint Security для Linux

   Подробнее о параметрах других программ безопасности см. в документации к этим программам.
4. Нажмите на кнопку **Сохранить**.

Изменения политики будут сохранены в свойствах политики и будут отображаться в разделе **История ревизий**.

Включение и выключение параметра наследования политики

Чтобы включить или выключить параметр наследования в политике:

1. Откройте требуемую политику.
2. Откройте закладку **Общие**.
3. Включите или выключите наследования политики:

- Если в дочерней группе включен параметр **Наследовать параметры родительской политики** и заблокированы некоторые параметры в родительской политике, тогда вы не можете изменить эти параметры политики для дочерней группы.

- Если в дочерней политике выключен параметр **Наследовать параметры родительской политики**, тогда вы можете изменить все параметры в дочерней политике, даже если некоторые параметры "заблокированы" в родительской политике.

- Если в родительской группе включен параметр **Обеспечить принудительное наследование параметров для дочерних политик**, то включается и 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 отклонить изменения.

По умолчанию, параметр **Наследовать параметры родительской политики** включен для новой политики.

Если у политики имеются профили, все дочерние политики наследуют эти профили.

Копирование политики

Вы можете копировать политики из одной группы администрирования в другую.

Чтобы скопировать политику в другую группу администрирования:

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется скопировать.
3. Нажмите на кнопку **Копировать**.

   В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу, то есть группу, в которую вы хотите скопировать политику (или политики).
5. Нажмите на кнопку **Копировать** внизу экрана.
6. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Политика (политики) и все ее профили скопированы в целевую группу администрирования. Каждая скопированная политика в целевой группе принимает статус **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Перемещение политики

Вы можете перемещать политики из одной группы администрирования в другую. Например, вы хотите удалить одну группу администрирования, но использовать ее политики для другой группы администрирования. В этом случае вам может потребоваться, перед удалением старой группы администрирования, переместить политику из старой группы администрирования в новую.

Чтобы переместить политику в другую группу администрирования:

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Установите флажок напротив политики (или политик), которую требуется переместить.
3. Нажмите на кнопку **Переместить**.

   В правой части экрана отображается дерево групп администрирования.
4. В дереве выберите целевую группу администрирования, то есть группу, в которую вы хотите переместить политику (или политики).
5. Нажмите на кнопку **Переместить** внизу 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 **Активна** в любое время.

   Если политика унаследована из группы источника, она останется в группе источника. Политика скопирована в целевую группу со всеми ее профилями. Статус политики в целевой группе администрирования будет **Неактивна**. Вы можете изменить статус политики на **Активна** в любое время.

Если в целевой группе политик уже существует политика с именем, совпадающим с именем копируемой политики, к имени копируемой политики будет добавлено окончание вида (<следующий порядковый номер>), например: (1).

Принудительная синхронизация

Несмотря на то, что Kaspersky Security Center Linux 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. Перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Нажмите на кнопку **Синхронизировать принудительно**.

Программа выполняет синхронизацию выбранного устройства с Сервером администрирования.

Синхронизация нескольких устройств

Чтобы осуществить принудительную синхронизацию между Сервером администрирования и несколькими управляемыми устройствами:

1. Откройте список устройств группы администрирования или выборку устройств:
   - В главном меню перейдите в раздел **Устройства** → **Управляемые устройства**, перейдите по ссылке в поле **Текущий путь** над списком управляемых устройств и выберите группу администрирования, в которую входят устройства для синхронизации.
   - Запустите выборку устройств, чтобы просмотреть список устройств.
2. Установите флажки рядом с устройствами, которые требуется синхронизировать с Сервером администрирования.
3. Над списком управляемых устройств нажмите на кнопку с многоточием (•••) и нажмите на кнопку **Синхронизировать принудительно**.

   Программа выполняет синхронизацию выбранных устройств с Сервером администрирования.
4. В списке устройств проверьте, что время последнего подключения к Серверу администрирования для выбранных устройств изменилось на текущее время. Если время не изменилось, обновите содержимое страницы, нажав на кнопку **Обновить**.

Выбранные устройства синхронизированы с Сервером администрирования.

Просмотр времени доставки политики

После изменения политики для программы "Лаборатории Касперского" на Сервере администрирования администратор может проверить, доставлена ли измененная политика на определенные управляемые устройства. Политика может быть доставлена во время регулярной или принудительной синхронизации.

Чтобы просмотреть дату и время доставки политики программы на управляемые устройства:

1. Перейдите в раздел **Устройства** → **Управляемые устройства**.
2. Выберите имя устройства, которое требуется синхронизировать с Сервером администрирования.

   В открывшемся окне свойств выберите раздел **Общие**.
3. Выберите закладку **Программы**.
4. Выберите программу, для которой требуется посмотреть дату синхронизации политики.

   Откроется окно политики программы, с выбранным разделом **Общие**, и отобразится дата и время доставки политики.

Просмотр диаграммы состояния применения политики

В Kaspersky Security Center вы можете просматривать состояние применения политики на каждом устройстве на диаграмме.

Чтобы просмотреть статус применения политики на каждом устройстве:

1. Перейдите в раздел **Устройства** → **Политики и профили политик**.
2. Установите флажок рядом с именем политики, для которой вы хотите просмотреть состояние применения на устройстве.

3. В появившемся меню выберите ссылку **Результаты применения**.

   Откроется окно **Результат распространения <название политики>**.

4. В открывшемся окне **Результат распространения <название политики>** отображается **Описание статуса**.

Вы можете изменить количество результатов, отображаемых в списке результатов применения политики. Максимальное количество устройств равно 100,000.

Чтобы изменить количество устройств, отображаемых в списке с результатами применения политики:

1. В панели инструментов перейдите в раздел **Параметры интерфейса**.
2. В поле **Максимальное количество устройств, отображаемых в результатах распространения политики** введите количество устройств (до 100 000).

   По умолчанию количество устройств равно 5000.

3. Нажмите на кнопку **Сохранить**.

   Параметры сохранены и применены.

Удаление политики

Вы можете удалить политику, если она больше не нужна. Вы можете удалить только неунаследованную политику в выбранной группе администрирования. Если политика унаследована, вы можете удалить ее только в группе администрирования, в которой она была создана.

Чтобы удалить политику:

1. В главном окне программы перейдите в раздел **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.

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.

Просмотр профилей политики

Чтобы просмотреть профили политики:

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.
2. Выберите политику, профили которой требуется просмотреть.

   Откроется окно свойств политики на закладке **Общие**.

3. Откройте закладку **Профили политики**.

Профили политики отобразятся в виде таблицы. Если у политики нет профилей политики, отобразится пустая таблица.

Изменение приоритета профиля политики

Чтобы изменить приоритет профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На закладке **Профили политики** установите флажок рядом с профилем политики, для которого требуется изменить приоритет.
3. Установите профиль политики на новую позицию в списке с помощью кнопок **Повысить приоритет** или **Понизить приоритет**.

   Чем выше расположен профиль политики в списке, тем выше его приоритет.

4. Нажмите на кнопку **Сохранить**.

Приоритет выбранного профиля политики изменен и применен.

Создание профиля политики

Чтобы создать профиль политики:

1. Перейдите к списку профилей выбранной политики.

   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. Выберите закладку **Параметры программы**.

   Можно также нажать на кнопку **Сохранить**, чтобы выйти. Созданный профиль политики отобразится в списке профилей политики, и вы сможете изменить его свойства позже.

5. В левой области закладки **Параметры программы** выберите нужный вам раздел и в панели результатов измените параметры профиля политики. Вы можете изменить параметры профиля политики в каждом разделе.

   Чтобы отменить изменения, вы можете нажать на кнопку **Отмена**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения профиля.

Профиль политики отобразится в списке профилей политики.

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.

   Откроется список профилей политики. Если у политики нет профилей политики, отобразится пустая таблица.

2. На закладке **Профили политики** 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.

Создание правила активации профиля политики

Развернуть все | Свернуть все

Чтобы создать правило активации профиля политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На закладке **Профили политики** нажмите на профиль политики, для которого требуется создать правило активации.

   Если список профилей политики пуст, вы можете создать профиль политики.

3. На закладке **Правила активации** нажмите на кнопку **Добавить**.

   Откроется окно с правилами активации профиля политики.

4. Укажите имя правила активации.

5. Установите флажки напротив условий, которые должны влиять на активацию создаваемого профиля политики:

   - **Общие правила активации профиля политики**

Установите флажок, чтобы настроить правила активации профиля политики на устройстве в зависимости от состояния автономного режима устройства, правила подключения устройства к Серверу администрирования и назначенных устройству тегов.

Для этого параметра на следующем шаге укажите:

- Статус устройства

  Определяет условие присутствия устройства в сети:
  - **В сети** – устройство находится в сети, Сервер администрирования доступен.
  - **Не в сети** – устройство находится во внешней сети, то есть Сервер администрирования недоступен.
  - **Неизвестно** – 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 выбранного владельца устройства**

  Для этого параметра на следующем шаге укажите:

  - Владелец устройства

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по владельцу устройства. В раскрывающемся списке под флажком можно выбрать критерий активации профиля:
    - устройство принадлежит указанному владельцу (знак "=");
    - устройство не принадлежит указанному владельцу (знак "#").

      Если параметр включен, активация профиля на устройстве выполняется в соответствии с настроенным критерием. Вы можете указать владельца устройства, когда параметр включен. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

  - Владелец устройства включен во внутреннюю группу безопасности

    Включите параметр, чтобы настроить и включить правило активации профиля на устройстве по членству владельца устройства во внутренней группе безопасности Kaspersky Security Center Linux. 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 Linux. Если параметр выключен, критерий активации профиля не применяется. По умолчанию параметр выключен.

- Правила для характеристик оборудования

  Установите флажок, чтобы настроить условие активации 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.

6. Проверьте список настроенных параметров. Если список верен, нажмите на кнопку **Создать**.

В результате профиль будет сохранен. Профиль будет активирован на устройстве, когда будут выполнены правила активации.

Правила активации профиля политики, созданные для профиля, отображаются в свойствах профиля политики на закладке **Правила активации**. Вы можете изменить или удалить правило активации профиля политики.

Несколько правил активации могут выполняться одновременно.

Удаление профиля политики

Чтобы удалить профиль политики:

1. Перейдите к списку профилей выбранной политики.

   Откроется список профилей политики.

2. На странице **Профили политики** установите флажок рядом с профилем политики, который вы хотите удалить, и нажмите на кнопку **Удалить**.

3. В появившемся окне нажмите на кнопку **Удалить** еще раз.

Профиль политики удален. Если политика наследуется группой более низкого уровня, профиль политики остается в этой группе, но становится профилем политики этой группы. Это позволяет уменьшить изменения в параметрах управляемых программ, установленных на устройствах групп нижнего уровня.

Пользователи и роли пользователей

В этом разделе описана работа с пользователями и ролями пользователей, а также приведены инструкции по их созданию и изменению, назначению пользователям ролей и групп и связи профилей политики с ролями.

О ролях пользователей

Роль пользователя (далее также *роль*) это объект, содержащий набор прав и разрешений. Роль может быть связана с параметрами программ "Лаборатории Касперского", которые установлены на устройстве пользователя. Вы можете назначить роль набору пользователей или набору групп на любом уровне иерархии групп администрирования.

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 каждой программы "Лаборатории Касперского" отдельно. Роль связана со многими профилями политики, которые созданы для разных программ. Таким образом, роль – это метод объединения параметров для определенного типа пользователя.

Настройка прав доступа к функциям программы. Управление доступом на основе ролей

Kaspersky Security Center Linux предоставляет доступ на основе ролей к функциям Kaspersky Security Center Linux и к функциям управляемых программ "Лаборатории Касперского".

Вы можете настроить права доступа к функциям программы для пользователей Kaspersky Security Center Linux одним из следующих способов:

- настраивать права каждого пользователя или группы пользователей индивидуально;
- создавать типовые роли пользователей с заранее настроенным набором прав и присваивать роли пользователям в зависимости от их служебных обязанностей.

Применение ролей пользователей облегчает и сокращает рутинные действия по настройке прав доступа пользователей к программе. Права доступа в роли настраивают в соответствии с типовыми задачами и служебными обязанностями пользователей.

Ролям пользователя можно давать названия, соответствующие их назначению. В программе можно создавать неограниченное количество ролей.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права.

Права доступа к функциям программы

В таблице ниже приведены функции Kaspersky Security Center Linux 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**, **Изменение** и **Выполнение** применимы к любой задаче, отчету или параметрам. В дополнение к этим правам у пользователя должно быть право **Выполнение операций с выборками устройств** для управления задачами, отчетами или изменения параметров выборок устройств.

Все задачи, отчеты, параметры и инсталляционные пакеты, отсутствующие в таблице, относятся к области **Общий функционал: Базовая функциональность**.

Права доступа к функциям программы

Функциональная область	Право	Действие пользователя: право, необходимое для выполнения действия	Задача	Отчет
Общие функции: **Управление группами администрирования**	**Изменение.**	• 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.
Общие функции: **Доступ к объектам независимо от их списков ACL**	**Чтение.**	Получение доступа на чтение ко всем объектам: **Чтение**.	Отсутствует.	Отсутствует.
Общий функционал: **Базовая функциональность**	• **Чтение.** • **Изменение.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	• Правила перемещения устройства (создание, изменение или удаление) для виртуального Сервера: **Изменение**, **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. • Распространять инсталляционные пакеты. • Установка программ на подчиненные Серверы администрирования.	• Отчет о сост защиты. • Отчет об угр • Отчет о наиб заражаемых устройствах • Отчет о стат антивирусны • Отчет об ош • Отчет о сете атаках. • Сводный отч программах защиты пери • Сводный отч типах установленн программ. • Отчет о пользовател зараженных устройств. • Отчет об инцидентах. • Отчет о соб

				• Отчет о рабо точек распростран • Отчет о подчиненны Серверах администри • Отчет о соб Контроля ус • Отчет о запрещенны программах. • Отчет о рабо Веб-Контрол • Отчет об эффективны правах пользовател • Отчет о прав
Общие функции: **Удаленные объекты**	• **Чтение.** • **Изменение.**	• Просмотр удаленных объектов в корзине: **Чтение**. • Удаление объектов из корзины: **Запись**.	Отсутствует.	Отсутствует.
Общие функции: **Обработка событий**	• **Удаление событий.** • **Изменение параметров уведомления о событиях.** • **Изменение параметров записи событий в журнал событий.** • **Изменение.**	• 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.
Общие функции: **Операции с Сервером администрирования**	• **Чтение.** • **Изменение.** • **EXECUTE.** • **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: **Изменение**. • Изменение SSL-портов Сервера администрирования для	• Резервное копирование данных Сервера администрирования. • Обслуживание базы данных.	Отсутствует.

		подключения с помощью Kaspersky Security Center Web Console: **Изменение**. • Изменение портов Сервера администрирования для подключения мобильных устройств: **Изменение**. • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования: **Изменение**. • Укажите максимальное количество событий, которое может отправлять Сервер администрирования: **Изменение**. • Изменение периода, в течение которого Сервер администрирования может отправлять события: **Изменение**.		
Общие функции: **Развертывание программ "Лаборатории Касперского"**	• **Управление патчами "Лаборатории Касперского".** • **Чтение.** • **Изменение.** • **Выполнение.** • **Выполнение действий над выборками устройств.**	Одобрить или отклонить установку патча: **Управление патчами "Лаборатории Касперского".**	Отсутствует.	• Отчет об использован лицензионны ключей виртуальным Сервером администрир • Отчет о верс программ "Лаборатори Касперского • Отчет о несовмести программах. • Отчет о верс обновлений модулей про "Лаборатори Касперского • Отчет о развертыван защиты.
Общие функции: **Управление лицензионными ключами**	• **Экспорт файл ключа.** • **Изменение.**	• Экспорт файл ключа: **Экспорт файл ключа.** • Изменение параметров лицензионного ключа Сервера администрирования: **Изменение**.	Отсутствует.	Отсутствует.
Общие функции: **Управление отчетами**	• **Чтение.** • **Изменение.**	• Создание отчетов для объектов независимо от их списков ACL: **Запись**. • Выполнять отчеты независимо от их списков ACLs: **Чтение**.	Отсутствует.	Отсутствует.
Общие функции: **Иерархия Серверов администрирования**	**Настройка иерархии Серверов администрирования**	• Добавление, обновление или удаление подчиненных Серверов администрирования: **Настройка иерархии Серверов администрирования**	Отсутствует.	Отсутствует.

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 ACL объекта.**	Отсутствует.	Отсутствует.
Общие функции: **Виртуальные Серверы администрирования.**	• **Управление виртуальными Серверами администрирования.** • **Чтение.** • **Изменение.** • **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.

Предопределенные роли пользователей

Роли пользователей, назначенные пользователям Kaspersky Security Center Linux, предоставляют им набор прав доступа к функциям программы.

Вы можете использовать предопределенные роли пользователей с уже настроенным набором прав или создавать роли и самостоятельно настраивать необходимые права. Некоторые из предопределенных пользовательских ролей, доступных в Kaspersky Security Center Linux, 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.

Примеры ролей для определенных должностей

Роль	Комментарий
Аудитор	Разрешено выполнение любых операций со всеми типами отчетов, а также всех операций просмотра, включая просмотр удаленных объектов (предоставлены права **Чтение** и **Запись** для области **Удаленные объекты**). Другие операции не разрешены. Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Контролер	Разрешен просмотр всех операций, не разрешены другие операции. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.
Специалист по безопасности	Разрешены всех операции просмотра, разрешено управление отчетами; предоставлены ограниченные права в области **Управление системой**: **Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.

В таблице ниже приведены права для каждой предопределенной роли пользователя.

Возможности функциональной области **Управление мобильными устройствами: Общие** и **Управление системой** недоступны в Kaspersky Security Center Linux. Пользователь с ролями **Администратор Системного администрирования**/**Оператор** и **Администратор управления мобильными устройствами**/**Оператор** имеют права доступа только в функциональной области **Общий функционал**: **Базовая функциональность**.

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.**
Оператор Сервера администрирования	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Виртуальные Серверы администрирования.**
Аудитор	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Доступ к объектам независимо от их списков ACL.** • **Удаленные объекты.** • **Управление отчетами.** Вы можете назначить эту роль сотруднику, который выполняет аудит вашей организации.
Администратор установки программ	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание программ "Лаборатории Касперского".** • **Управление лицензионными ключами.** Предоставляет права на **Чтение** и **Выполнение** в области **Общий функционал: Виртуальные Серверы администрирования**.
Оператор установки программ	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: **Общий функционал**: • **Базовая функциональность.** • **Развертывание программ "Лаборатории Касперского"** (также предоставляет права на **Управление патчами "Лаборатории Касперского"** в этой же области). • **Виртуальные Серверы администрирования.**
Администратор Kaspersky Endpoint Security	Разрешает все операции в следующих функциональных областях: • **Общий функционал: Базовая функциональность.** • Область Kaspersky Endpoint Security, включая все функции.
Оператор Kaspersky Endpoint Security	Предоставляет права на **Чтение** и **Выполнение** во всех следующих функциональных областях: • **Общий функционал: 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.**

Главный оператор	Предоставляет права на **Чтение** и **Выполнение** (если применимо) во всех следующих функциональных областях: • **Общие функции**: • **Базовая функциональность.** • **Удаленные объекты.** • **Операции с Сервером администрирования.** • **Развертывание программ "Лаборатории Касперского".** • **Виртуальные Серверы администрирования.** • Область Kaspersky Endpoint Security, включая все функции.
Администратор управления мобильными устройствами	Разрешает все операции в области **Общий функционал: функциональная область Базовая функциональность**.
Специалист по безопасности	Разрешает все операции в следующих функциональных областях: **Общий функционал**: • **Доступ к объектам независимо от их списков ACL.** • **Управление отчетами.** Предоставляет права на **Чтение**, **Изменение**, **Выполнение**, **Сохранение файлов с устройств на рабочем месте администратора** и **Выполнение операций с выборками устройств** в области **Управление системой: Подключения**. Вы можете назначить эту роль сотруднику, который отвечает за IT-безопасность в вашей организации.
Пользователь Self Service Portal	Разрешает все операции в области **Управление мобильными устройствами: Self Service Portal**. Эта функция не поддерживается в версиях программы Kaspersky Security Center 11 и выше.
Контролер	Предоставляет права на **Чтение** в области **Общий функционал**: **Доступ к объектам независимо от их списков ACL** и О**бщий функционал**: функциональная область **Управление отчетами**. Вы можете назначить эту роль специалисту по безопасности и другим менеджерам, которые отвечают за IT-безопасность в вашей организации.

Добавление учетной записи внутреннего пользователя

Чтобы добавить новую учетную запись пользователя Kaspersky Security Center Linux:

1. В главном окне программы перейдите в раздел **Пользователи и роли** 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 Linux.
     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A–Z);
       - нижний регистр (a–z);
       - 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".

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.

Создание группы безопасности

Чтобы создать группу безопасности:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новый объект** выберите **Группа**.
4. Укажите следующие параметры группы безопасности:
   - **Имя группы**
   - **Описание**
5. Нажмите на кнопку **ОК**, чтобы сохранить изменения.

Созданная группа безопасности отобразится в списке пользователей и групп безопасности.

Изменение учетной записи внутреннего пользователя

Чтобы изменить учетную запись внутреннего пользователя Kaspersky Security Center Linux:

1. В главном окне программы перейдите в раздел **Пользователи и роли** и выберите вкладку **Пользователи**.
2. Выберите учетную запись пользователя, которую требуется изменить.
3. В открывшемся окне на закладке **Общие** измените параметры учетной записи пользователя:
   - **Описание**
   - **Полное имя**
   - **Адрес электронной почты**
   - **Основной телефон**
   - **Задать новый пароль** для подключения пользователя к Kaspersky Security Center Linux.
     Пароль должен соответствовать следующим правилам:
     - Длина пароля должна быть от 8 до 16 символов.
     - Пароль должен содержать символы как минимум трех групп списка ниже:
       - верхний регистр (A–Z);
       - нижний регистр (a–z);
       - 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 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 **Выключено**, чтобы запретить пользователю подключаться к программе. Например, можно отключить учетную запись после того, как сотрудник увольняется из компании.

4. На закладке **Проверка подлинности** вы можете указать параметры безопасности для этой учетной записи.
5. На закладке **Группы** можно добавить пользователя или группу безопасности.
6. На закладке **Устройства** можно назначить устройства пользователю.
7. На закладке **Роли** можно назначить роль пользователю.
8. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная учетная запись пользователя отобразится в списке пользователей.

Изменение группы безопасности

Можно изменять только внутренние группы.

Чтобы изменить группу безопасности:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Выберите группу безопасности, которую требуется изменить.
3. В открывшемся окне измените параметры группы безопасности:
   - **Имя**
   - **Описание**
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная учетная запись пользователя отобразится в списке пользователей и групп безопасности.

Добавление учетных записей пользователей во внутреннюю группу

Учетные записи внутренних пользователей можно добавлять только во внутреннюю группу.

Чтобы добавить учетные записи пользователей в группу:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Установите флажки напротив учетных записей пользователей, которые требуется добавить в группу.
3. Нажмите на кнопку **Назначить группу**.
4. В открывшемся окне **Назначить группу** выберите группу, в которую требуется добавить учетные записи пользователей.
5. Нажмите на кнопку **Назначить**.

Учетные записи пользователей добавлены в группу.

Назначение пользователя владельцем устройства

Информацию о назначении пользователя владельцем мобильного устройства см. в справке Kaspersky Security для мобильных устройств.

Чтобы назначить пользователя владельцем устройства:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Нажмите на учетную запись пользователя, которую требуется назначить в качестве владельца устройству.
3. В открывшемся окне свойств пользователя выберите закладку **Устройства**.
4. Нажмите на кнопку **Добавить**.
5. Из списка устройств выберите устройство, которое вы хотите назначить пользователю.
6. Нажмите на кнопку **ОК**.

Выбранное устройство добавляется в список устройств, назначенных пользователю.

Также можно выполнить эту операцию в группе **Устройства** → **Управляемые устройства**, выбрав имя устройства, которое вы хотите назначить, и перейдя по ссылке **Назначить нового владельца**.

Удаление пользователей или групп безопасности

Можно удалять только внутренних пользователей или группы безопасности.

Удаление пользователей или групп безопасности:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Установите флажок рядом с именем пользователя или группы безопасности, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**.

Пользователь или группа безопасности удалены.

Создание роли пользователя

Чтобы создать роль пользователя:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Имя новой роли** укажите имя новой роли.
4. Нажмите на кнопку **ОК**, чтобы применить изменения.
5. В открывшемся окне измените параметры роли:
   - На закладке **Общие** измените имя роли.
     Вы не можете изменять имена типовых ролей.
   - На закладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
   - На закладке **Права доступа** измените права доступа к программам "Лаборатории Касперского".
6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Созданная роль появится в списке ролей пользователей.

Изменение роли пользователя

Чтобы изменить роль пользователя:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется изменить.
3. В открывшемся окне измените параметры роли:
   - На закладке **Общие** измените имя роли.

Вы не можете изменять имена типовых ролей.

- На закладке **Параметры** измените область действия роли, а также политики и профили политик, связанные с ролью.
- На закладке **Права доступа** измените права доступа к программам "Лаборатории Касперского".

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Обновленная роль появится в списке ролей пользователей.

Изменение области для роли пользователя

Область роли пользователя – это комбинация пользователей и групп администрирования. Параметры, связанные с ролью пользователя, применяются только к устройствам, принадлежащим тем пользователям, которым назначена эта роль, и только если эти устройства принадлежат к группам, которым назначена эта роль, включая дочерние группы.

Чтобы добавить пользователей, группы безопасности и группы администрирования в область роли пользователя, воспользуйтесь одним из следующих способов:

Способ 1:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Пользователи**.
2. Установите флажки напротив имен пользователей и групп безопасности, которые требуется добавить в область роли.
3. Нажмите на кнопку **Назначить роль**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
4. На 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 программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, для которой требуется задать область.
3. В открывшемся окне свойств роли выберите закладку **Параметры**.
4. В разделе **Область действия роли** нажмите на кнопку **Добавить**.

   Будет запущен мастер назначения роли. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На 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. Закройте окно свойств роли.

Выбранные пользователи, группы безопасности и группы администрирования добавлены в область роли.

Способ 3:

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 вы хотите добавить область пользовательской роли, и нажмите на кнопку **Роли**.

   Вы не можете выбрать несколько пользователей или групп безопасности одновременно. Если вы выберете более одного объекта, кнопка **Роли** будет неактивна.
3. В окне **Роли** выберите пользовательскую роль, которую вы хотите назначить, и нажмите на кнопку **OK**, чтобы сохранить изменения.

   Выбранные пользователи или группы безопасности добавлены в область роли.

Удаление роли пользователя

Чтобы удалить роль пользователя:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Установите флажок напротив роли, которую требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Роль пользователя будет удалена.

Связь профилей политики с ролями

Вы можете связывать роли с профилями политик. В этом случае правило активации для профиля политики определяется в зависимости от роли: профиль политики становится активным для пользователя с определенной ролью.

Например, политика запрещает запуск программ городской навигации для всех устройств группы администрирования. Программы городской навигации необходимы для работы только одного устройства пользователя, выполняющего роль курьера, в группе администрирования "Пользователи". В этом случае можно назначить роль "Курьер" владельцу этого устройства и создать профиль политики, разрешающий использовать программы городской навигации на устройствах, владельцам которых назначена роль "Курьер". Все остальные параметры политики остаются без изменений. Только пользователям с ролью "Курьер" разрешено использовать программы городской навигации. Затем, если другому сотруднику будет назначена роль "Курьер", этот сотрудник также сможет использовать программы городской навигации на устройстве, принадлежащем вашей организации. Однако использование программ городской навигации будет запрещено на других устройствах этой группы администрирования.

Чтобы связать роль с профилем политики:

1. В главном окне программы перейдите в раздел **Пользователи и роли** → **Роли**.
2. Выберите роль, которую требуется связать с профилем политики.

   Откроется окно свойств роли на закладке **Общие**.
3. Перейдите на закладку **Параметры** и прокрутите 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.

Распространение пользовательских ролей на подчиненные Серверы администрирования

По умолчанию списки пользовательских ролей главного и подчиненного Серверов администрирования являются независимыми. Вы можете настроить программы для автоматического распространения ролей пользователей, созданных на главном Сервере администрирования, на все подчиненные Сервера администрирования. Роли пользователей также могут распространяться с подчиненного Сервера администрирования на собственные подчиненные Сервера администрирования.

Чтобы распространить роли пользователей с главного Сервера администрирования на подчиненные Серверы администрирования:

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

Откроется окно свойств Сервера администрирования на закладке **Общие**.

2. Перейдите в раздел **Иерархия Серверов администрирования**.

3. Включите параметр **Передать список ролей подчиненному Серверу администрирования** и нажмите на кнопку **Сохранить**.

Программа копирует роли пользователей главного Сервера администрирования на подчиненные Серверы администрирования.

Если параметр **Передать список ролей подчиненному Серверу администрирования** включен и роли пользователей распространены, такие роли не доступны для изменений или удаления на подчиненном Сервере администрирования. Когда вы создаете роль или изменяете существующую роль на главном Сервере администрирования, изменения автоматически копируются на подчиненные Серверы администрирования. Когда вы удаляете роль пользователя на главном Сервере администрирования, эта роль остается на подчиненном Сервере администрирования и может быть изменена или удалена.

Роли, которые распространяются на подчиненный Сервер администрирования с главного Сервера, отображаются с помощью зеленого флажка (✓). Вы не можете изменять эти роли на подчиненном Сервере администрирования.

Если роль создается на главном Сервере администрирования, а на подчиненном Сервере администрирования есть роль с таким же именем, новая роль копируется на подчиненный Сервер администрирования, и к ее имени в скобках добавляется номер, например, ~~1, ~~2 (номер может быть случайным).

Если выключить параметр **Передать список ролей подчиненному Серверу администрирования**, все роли пользователя останутся на подчиненных Серверах администрирования, но станут независимыми от ролей на главном Сервере администрирования. Когда роли на подчиненных Серверах администрирования становятся независимыми, их можно изменять или удалять.

Работа с ревизиями объектов

Этот раздел содержит информацию о работе с ревизиями объектов. Kaspersky Security Center Linux позволяет отслеживать изменения объектов. Каждый раз, когда вы сохраняете изменения объекта, создается *ревизия*. Каждая ревизия имеет номер.

Объекты программы, которые поддерживают работу с ревизиями:

- Свойства Сервера администрирования
- Политики
- Задачи
- Группы администрирования
- Учетные записи пользователей
- Инсталляционные пакеты

Вы можете просмотреть список ревизий и откатить изменения, выполненные с объектом, до выбранной ревизии.

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.
- **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.

Откат изменений объекта к предыдущей ревизии

В случае необходимости вы можете откатить изменения объекта. Например, вам может понадобиться вернуть параметры политики к состоянию на определенную дату.

Чтобы откатить изменения объекта:

1. В окне свойств объекта перейдите на закладку **История ревизий**.

2. В списке ревизий объекта выберите ревизию, к которой нужно откатить изменения.

3. Нажмите на кнопку **Откатить**.

4. Нажмите на кнопку **OK**, 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.

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
- Пользователи
- 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** для области **Удаленные объекты**.

Об удалении клиентских устройств

При удалении управляемого устройства из группы администрирования программа перемещает устройство в группу Нераспределенные устройства. После удаления устройства установленные программы "Лаборатории Касперского" – Агент администрирования и программа безопасности, например Kaspersky Endpoint Security, – остаются на устройстве.

Kaspersky Security Center 14 Linux обрабатывает устройства из группы Нераспределенные устройства по следующим правилам:

- Если вы настроили правила перемещения устройств 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.

При удалении устройства из группы Нераспределенные устройства вручную программа удаляет устройство из списка. После удаления устройства установленные программы "Лаборатории Касперского" (если они есть) остаются на устройстве. Затем, если устройство по-прежнему видно Серверу администрирования и вы настроили регулярный опрос сети, Kaspersky Security Center 14 Linux 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.

Использование утилиты klscflag для открытия порта 13291

Вы можете автоматизировать работу Kaspersky Security Center с помощью утилиты klakaut. Утилита klakaut и справочная система для нее расположены в папке установки Kaspersky Security Center. 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`.

Использование утилиты klscflag для открытия порта OpenAPI

Порт OpenAPI используется программой Kaspersky Security Center 14 Web Console для подключения к Серверу администрирования. По умолчанию для порта OpenAPI указано значение 13299.

Чтобы открыть порт OpenAPI:

1. Выполните следующую команду в командной строке:
   ```
   $ /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_OPEN_OAPI_PORT -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 OpenAPI открыт.

Чтобы проверить, успешно ли открыт порт OpenAPI, выполните следующую команду в командной строке:

```
$ /opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_OPEN_OAPI_PORT -svt BOOL_T -ss "|ss_type
= \"SS_SETTINGS\";"
```

Эта команда возвращает следующий результат:

```
+--- (PARAMS_T)
+---KLSRV_SP_OPEN_OAPI_PORT = (BOOL_T)true
```

Значение `true` означает, что порт открыт. В противном случае отображается значение `false`.

Обновление баз и программ "Лаборатории Касперского"

В этом разделе описаны шаги, которые вы должны выполнить для регулярных обновлений:

- баз и программных модулей "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN могут быть недоступны в программе на территории США.

Сценарий: Регулярное обновление баз и программ "Лаборатории Касперского"

В этом разделе представлен сценарий регулярного обновления баз данных, программных модулей и программ "Лаборатории Касперского". После того, как вы завершили сценарий Настройка защиты в сети организации, вы должны поддерживать надежность системы защиты, чтобы обеспечить защиту Серверов администрирования и управляемых устройств от различных угроз, включая вирусы, сетевые атаки и фишинговые атаки.

Защита сети поддерживается обновленной с помощью регулярных обновлений следующего:

- баз и программных модулей "Лаборатории Касперского";
- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

Когда вы завершите этот сценарий, вы можете быть уверены, что:

- Ваша сеть защищена самым последним программным обеспечением "Лаборатории Касперского", включая компоненты Kaspersky Security Center Linux и программы безопасности.
- Антивирусные базы и другие базы данных "Лаборатории Касперского", критически важные для безопасности сети, всегда актуальны.

Предварительные требования

Управляемые устройства должны иметь соединение с Сервером администрирования. Если у устройств нет соединения, рассмотрите возможность обновления баз, программных модулей и программ "Лаборатории Касперского" вручную или напрямую с серверов обновлений "Лаборатории Касперского".

Сервер администрирования должен иметь подключение к интернету.

Прежде чем приступать, убедитесь, что вы выполнили следующее:

1. Развернуты программы безопасности "Лаборатории Касперского" на управляемых устройствах в соответствии со сценарием развертывания программ "Лаборатории Касперского" с помощью Kaspersky Security Center 14 Web Console.

2. Созданы и настроены все необходимые политики, профили политик и задачи в соответствии со сценарием настройки защиты сети.

3. Назначено соответствующее количество точек распространения в соответствии с количеством управляемых устройств и топологией сети.

Обновление баз и программ "Лаборатории Касперского" состоит из следующих этапов:

1 Выбор схемы обновления

Существует несколько схем, которые вы можете использовать для установки обновлений компонентов Kaspersky Security Center и программ безопасности. Выберите схему или несколько схем, которые лучше всего соответствуют требованиям вашей сети.

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.

Инструкции: Создание задачи для загрузки обновлений в хранилище Сервера администрирования.

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

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. Когда эта функция включена, Сервер администрирования или точка распространения загружает файлы различий вместо целых файлов баз данных или программных модулей "Лаборатории Касперского". Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Поэтому файлы различий занимают меньше места, чем целые файлы. В результате уменьшается трафик между Сервером администрирования или точками распространения и управляемыми устройствами. Чтобы использовать эту функцию, включите параметр **Загрузить файлы различий** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования* и/или *Загрузка обновлений в хранилища точек распространения*.

Инструкция: использование файлов различий для обновления баз и программных модулей "Лаборатории Касперского"

6 Настройка автоматической установки обновлений для программ безопасности

Создайте задачу *Обновление* для управляемых программ, чтобы обеспечить своевременное обновление программных модулей и баз данных "Лаборатории Касперского", в том числе антивирусных баз. Чтобы обеспечить своевременное обновление, рекомендуется при настройке расписания задачи выбрать вариант **При загрузке обновлений в хранилище**.

Если в вашей сети есть устройства, поддерживающие только IPv6, и вы хотите регулярно обновлять программы безопасности, установленные на этих устройствах, убедитесь, что на управляемых устройствах установлены Сервер администрирования версии 13.2 и Агент администрирования версии 13.2.

Если обновление требует принятия условий Лицензионного соглашения, сначала вам требуется прочитать и принять условия Лицензионного соглашения. После этого обновления могут быть распространены на управляемые устройства.

Результаты

После завершения сценария, Kaspersky Security Center Linux настроен на обновление баз "Лаборатории Касперского" после загрузки обновлений в хранилище Сервера администрирования. Теперь вы можете приступить к мониторингу состояния сети.

Об обновлении баз, программных модулей и программ "Лаборатории Касперского"

Чтобы убедиться, что защита ваших Серверов администрирования и управляемых устройств актуальна, вы должны своевременно предоставлять обновления следующего:

- баз и программных модулей "Лаборатории Касперского";

  Kaspersky Security Center проверяет доступность серверов "Лаборатории Касперского" перед загрузкой баз и программных модулей "Лаборатории Касперского". Если доступ к серверам через системный DNS невозможен, программа использует публичный DNS. Это необходимо для обновления антивирусных баз и поддержания уровня безопасности управляемых устройств.

- установленных программ "Лаборатории Касперского", включая компоненты Kaspersky Security Center и программ безопасности.

  Kaspersky Security Center не может обновлять программы "Лаборатории Касперского" автоматически. Чтобы обновить программы, загрузите последние версии программ с сайта "Лаборатории Касперского" и установите их вручную:

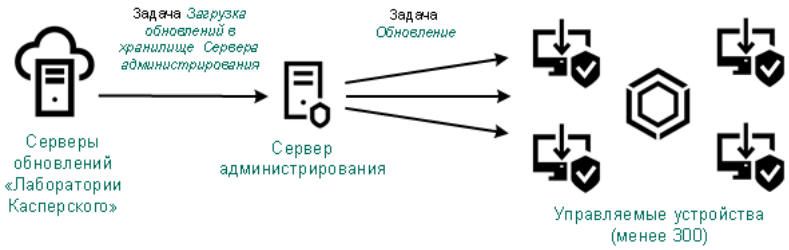
  - Сервер администрирования Kaspersky Security Center и Kaspersky Security Center 14 Web Console.
  - Агент администрирования, Kaspersky Endpoint Security для Linux, веб-плагин управления.

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 для Linux 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).



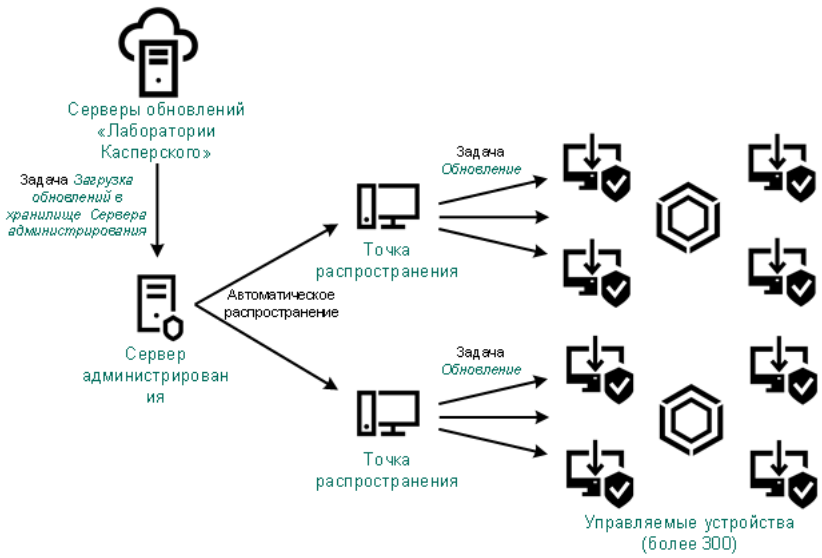
Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и без точек распространения

В качестве источника обновлений 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 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 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.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования с точками распространения

После выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования*, обновления баз "Лаборатории Касперского" и программные модули для Kaspersky Endpoint Security для Linux загружены в хранилище Сервера администрирования. Эти обновления устанавливаются с помощью задачи Обновление Kaspersky Endpoint Security для Linux.

Задача Загрузка обновлений в хранилище Сервера администрирования недоступна на виртуальных Серверах администрирования. В хранилище виртуального Сервера отображаются обновления, загруженные на главный Сервер администрирования.

Вы можете настроить проверку полученных обновлений на работоспособность и на наличие ошибок на наборе тестовых устройств. Если проверка прошла успешно, обновления распространяются на другие управляемые устройства.

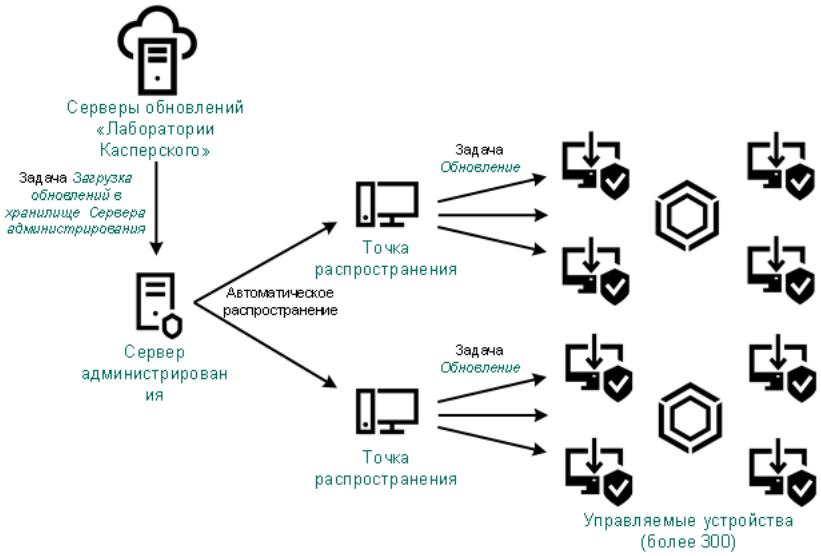
Каждая управляемая программа "Лаборатории Касперского" запрашивает требуемые обновления с Сервера администрирования. Сервер администрирования объединяет эти запросы и загружает только те обновления, которые запрашиваются программами. Это обеспечивает то, что загружаются только нужные обновления и только один раз. При выполнении задачи *Загрузка обновлений в хранилище Сервера администрирования*, для обеспечения загрузки необходимых версий баз и программных модулей "Лаборатории Касперского", на серверы обновлений "Лаборатории Касперского" автоматически, Сервер администрирования отправляет следующую информацию:

- идентификатор и версия программы;
- идентификатор установки программы;
- идентификатор активного ключа;
- идентификатор запуска задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Передаваемая информация не содержит персональных данных и других конфиденциальных данных. АО "Лаборатория Касперского" защищает полученную информацию в соответствии с установленными законом требованиями.

Использование двух задач: Загрузка обновлений в хранилище Сервера администрирования и Загрузка обновлений в хранилища точек распространения

Вы можете загружать обновления в хранилища точек распространения непосредственно с серверов обновлений "Лаборатории Касперского" вместо хранилища Сервера администрирования, а затем распространять обновления на управляемые устройства (см. рисунок ниже). Загрузка обновлений из хранилищ точек распространения предпочтительнее, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.



Обновление с использованием задачи Загрузка обновлений в хранилище Сервера администрирования и задачи Загрузка обновлений в хранилища точек распространения

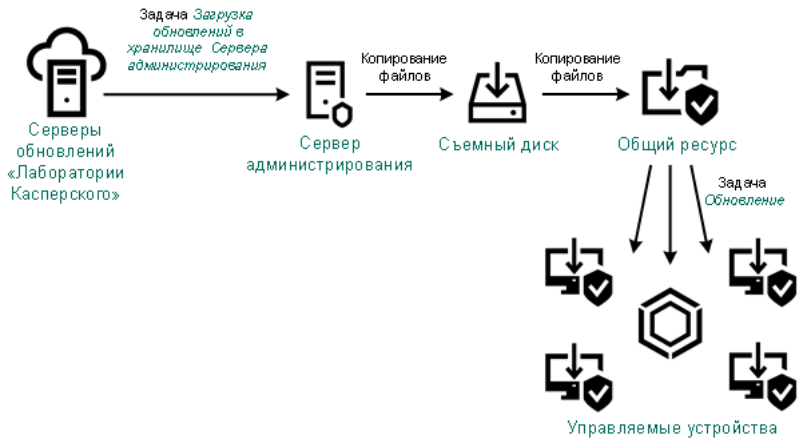
По умолчанию Сервер администрирования и точки распространения взаимодействуют с серверами обновлений "Лаборатории Касперского" и загружают обновления по протоколу HTTPS. Вы можете настроить Сервер администрирования и/или точки распространения на использование протокола HTTP вместо HTTPS.

Для реализации этой схемы создайте задачу *Загрузка обновлений в хранилища точек распространения* в дополнение к задаче *Загрузка обновлений в хранилище Сервера администрирования*. После этого точки распространения загружают обновления с серверов обновлений "Лаборатории Касперского", а не из хранилища Сервера администрирования.

Для этой схемы также требуется задача *Загрузка обновлений в хранилище Сервера администрирования*, так как эта задача используется для загрузки баз и программных модулей "Лаборатории Касперского" для Kaspersky Security Center.

Вручную через локальную папку, общую папку или FTP-сервер

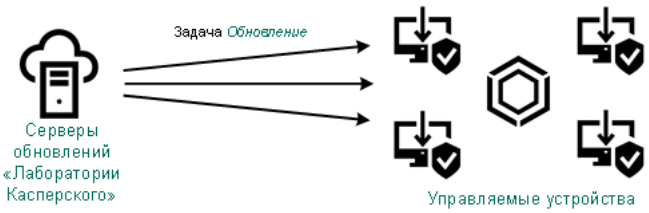
Если клиентские устройства не подключены к Серверу администрирования, вы можете использовать локальную папку или общий ресурс в качестве источника обновления баз, программных модулей и программ "Лаборатории Касперского". В этой схеме вам нужно скопировать необходимые обновления из хранилища Сервера администрирования на съемный диск, а затем скопировать обновления в локальную папку или общий ресурс, указанный в качестве источника обновлений в параметрах Kaspersky Endpoint Security для Linux (см. рисунок ниже).



Обновление через локальную папку, общую папку или FTP-сервер

Непосредственно с серверов обновлений "Лаборатории Касперского" для Kaspersky Endpoint Security для Linux на управляемых устройствах

На управляемых устройствах вы можете настроить Kaspersky Endpoint Security для Linux на получение обновлений напрямую с серверов обновлений "Лаборатории Касперского" (см. рисунок ниже).



Обновление программ безопасности непосредственно с серверов обновлений "Лаборатории Касперского"

В этой схеме программа безопасности не использует хранилище, предоставленное Kaspersky Security Center. Чтобы получать обновления непосредственно с серверов обновлений "Лаборатории Касперского", укажите серверы обновлений "Лаборатории Касперского" в качестве источника обновлений в программе безопасности. Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Linux.

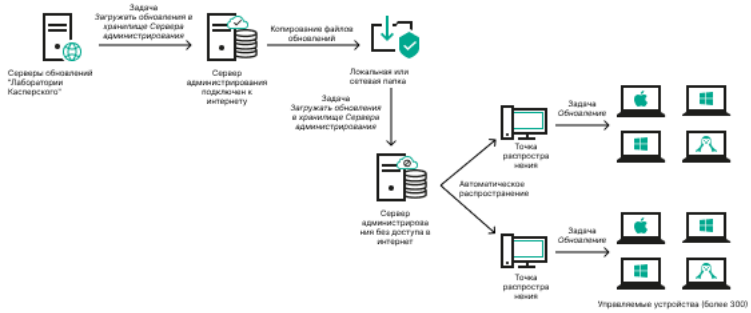
Через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

Если Сервер администрирования не имеет подключения к интернету, вы можете настроить задачу *Загрузка обновлений в хранилище Сервера администрирования* для загрузки обновлений из локальной или сетевой папки. В этом случае требуется время от времени копировать необходимые файлы обновлений в указанную папку. Например, вы можете скопировать необходимые файлы обновления из одного из следующих источников:

- Сервер администрирования, имеющий выход в интернет (см. рис. ниже).

  Так как Сервер администрирования загружает только те обновления, которые запрашиваются программами безопасности, наборы программ безопасности, которыми управляют Серверы администрирования (подключенные и не подключенные к интернету) должны совпадать.

  Если Сервер администрирования, который вы используете для загрузки обновлений, имеет версию 13.2 или более раннюю, откройте свойства задачи *Загрузка обновлений в хранилище Сервера администрирования*, а затем включите параметр **Загружать обновления, используя старую схему**.



Обновление через локальную или сетевую папку, если Сервер администрирования не имеет доступа в интернет

- Kaspersky Update Utility

  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*.

Создание задачи Загрузка обновлений в хранилище Сервера администрирования

Развернуть все | Свернуть все

Задача *Загрузка обновлений в хранилище Сервера администрирования* позволяет загружать обновления баз и программных модулей программы безопасности "Лаборатории Касперского" с серверов обновлений "Лаборатории Касперского" в хранилище Сервера администрирования.

Мастер первоначальной настройки Kaspersky Security Center автоматически создает задачу Сервера администрирования *Загрузка обновлений в хранилище Сервера администрирования*. 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*. Это позволяет убедиться, что Сервер администрирования правильно установит загруженные обновления и уровень безопасности не снизится из-за обновлений. Чтобы проверить обновления перед распространением, настройте параметр **Выполнить проверку обновлений** в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы создать задачу Загрузка обновлений в хранилище Сервера администрирования:

1. Перейдите в раздел **Устройства** → **Задачи**.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. Для программы Kaspersky Security Center выберите тип задачи **Загрузка обновлений в хранилище Сервера администрирования**.

4. Укажите имя задачи, которую вы создаете. Имя задачи не может превышать 100 символов и не может содержать специальные символы ("*<>?\:|).

5. На странице **Завершение создания задачи**, можно включить параметр **Открыть окно свойств задачи после ее создания**, чтобы открыть окно свойств задачи и изменить параметры задачи по умолчанию. Также можно настроить параметры задачи позже в любое время.

6. Нажмите на кнопку **Готово**.

   Задача будет создана и отобразится в списке задач.

7. Чтобы открыть окно свойств задачи, нажмите на имя созданной задачи.

8. В окне свойств задачи на закладке **Параметры программы** укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений можно использовать серверы обновлений "Лаборатории Касперского", локальную или сетевую папку или главный Сервер администрирования.

     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.

   - **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.

     По умолчанию параметр выключен.

   - **Загружать обновления, используя старую схему**

     Начиная с версии 14, Kaspersky Security Center загружает обновления баз и программных модулей по новой схеме. Чтобы программа могла загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

     Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих программ:

     - Kaspersky Update Utility

       Эта утилита загружает обновления по старой схеме.

- Kaspersky Security Center 13 Linux

  Например, один Сервер администрирования не имеет подключения к интернету. В этом случае можно загружать обновления с помощью второго Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную или сетевую папку, чтобы использовать ее в качестве источника обновлений для первого Сервера. Если второй Сервер администрирования имеет номер версии 13, включите параметр **Загружать обновления, используя старую схему** в задаче для первого Сервера администрирования.

По умолчанию параметр выключен.

- **Выполнить проверку обновлений**

  Если флажок установлен, Сервер администрирования копирует обновления из источника, сохраняет их во временном хранилище и запускает задачу Проверка обновлений, указанную в поле **Задача проверки обновлений**. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования и распространяются на устройства, для которых Сервер администрирования является источником обновлений (запускаются задачи с типом расписания **При загрузке обновлений в хранилище**). Задача загрузки обновлений в хранилище считается завершенной только после завершения задачи *Проверка обновлений*.

  По умолчанию параметр выключен.

9. В окне свойств задачи на закладке **Расписание** создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию**:

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Вручную** (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 программой, для которой вы создаете задачу.

    По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

  - **Каждую N неделю**

    Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

    По умолчанию задача запускается каждую пятницу в текущее системное время.

  - **Ежедневно (не поддерживается 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 Linux.

    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. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам.

- Дополнительные параметры задачи:

  - **Запускать пропущенные задачи**

    Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

    Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

    Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. 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 задачи**

    Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

    Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  - **Использовать случайную задержку запуска задачи в интервале (мин)**

    Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

    Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

    По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

- **Остановить задачу, если она выполняется более чем (мин)**

  По истечении заданного времени задача останавливается автоматически, независимо от того, завершена она или нет.

  Включите этот параметр, если вы хотите прервать (или остановить) задачи, которые слишком долго выполняются.

  По умолчанию параметр выключен. Время выполнения задачи по умолчанию – 120 минут.

10. Нажмите на кнопку **Сохранить**.

    Задача создана и настроена.

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа Сервера администрирования. Если задача создается для группы администрирования, то она распространяется только на Агенты администрирования, входящие в указанную группу администрирования.

Из папки общего доступа обновления распространяются на клиентские устройства и подчиненные Серверы администрирования.

Просмотр полученных обновлений

В результате выполнения задачи *Загрузка обновлений в хранилище Сервера администрирования* обновления баз и программных модулей копируются с источника обновлений и размещаются в папке общего доступа Сервера администрирования. Просмотреть загруженные обновления можно в разделе **Обновления баз и программных модулей "Лаборатории Касперского"**.

Чтобы просмотреть список полученных обновлений,

В главном окне программы перейдите в раздел **Операции → Программы "Лаборатории Касперского" → Обновления баз и программных модулей "Лаборатории Касперского"**.

Отобразится список доступных обновлений.

Проверка полученных обновлений

Развернуть все | Свернуть все

Перед установкой обновлений на управляемые устройства вы можете сначала проверить их на работоспособность и ошибки с помощью задачи *Проверка обновлений*. Задача *Проверка обновлений* выполняется автоматически в рамках задачи *Загрузка обновлений в хранилище Сервера администрирования*. Сервер администрирования загружает обновления с источника, сохраняет их во временном хранилище и запускает задачу *Проверка обновлений*. В случае успешного выполнения этой задачи обновления копируются из временного хранилища в папку общего доступа Сервера администрирования. Обновления распространяются на клиентские устройства, для которых Сервер администрирования является источником обновления.

Если по результатам выполнения задачи *Проверка обновлений* размещенные во временном хранилище обновления признаны некорректными или задача завершается с ошибкой, копирование обновлений в папку общего доступа не производится. На Сервере администрирования остается предыдущий набор обновлений. Запуск задач с типом расписания **При загрузке обновлений в хранилище** также не выполняется. Эти операции выполняются при следующем запуске задачи *Загрузка обновлений в хранилище Сервера администрирования*, если проверка нового набора обновлений завершится успешно.

Набор обновлений считается некорректным, если хотя бы на одном из тестовых устройств выполняется одно из следующих условий:

- произошла ошибка выполнения задачи обновления;
- после применения обновлений изменился статус постоянной защиты программы безопасности;
- в ходе выполнения задачи проверки по требованию был найден зараженный объект;
- произошла ошибка функционирования программы "Лаборатории Касперского".

Если ни одно из перечисленных условий ни на одном из тестовых устройств не выполняется, набор обновлений признается корректным и задача *Проверка обновлений* считается успешно выполненной.

Прежде чем приступить к созданию задачи *Проверка обновлений*, выполните предварительные условия:

1. Создайте группу администрирования с несколькими тестовыми устройствами. 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 вирусов для какой-нибудь программы, которую поддерживает Kaspersky Security Center, например, Kaspersky Endpoint Security для Linux. При создании задач обновления и поиска вирусов укажите группу администрирования с тестовыми

устройствами.

Задача *Проверка обновлений* последовательно запускает задачи обновления и поиска вирусов на тестовых устройствах, чтобы убедиться, что все обновления актуальны. Также при создании задачи *Проверка обновлений* необходимо указать задачи обновления и поиска вирусов.

3. Создайте задачу *Загрузка обновлений в хранилище Сервера администрирования*.

Чтобы Kaspersky Security Center Linux проверял полученные обновления перед распространением их на клиентские устройства:

1. В главном окне программы перейдите в раздел **Устройства → Задачи**.
2. Нажмите на имя задачи **Загрузка обновлений в хранилище Сервера администрирования**.
3. В открывшемся окне свойств задачи перейдите на закладку **Параметры программы** и включите параметр **Выполнить проверку обновлений**.
4. Если задача *Проверка обновлений* существует, нажмите на кнопку **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 вирусов.

      После этого появляются следующие параметры. Рекомендуется оставить их включенными:

      - **Перезагружать устройство после обновления баз**

        После обновления антивирусных баз на устройстве рекомендуется перезагрузить устройство.

        По умолчанию параметр включен.

      - **Проверять статус постоянной защиты после обновления баз и перезапуска устройства**

        Если этот параметр включен, задача *Проверка обновлений* проверяет, актуальны ли обновления, загруженные в хранилище Сервера администрирования, и не снизился ли уровень защиты после обновления антивирусных баз и перезагрузки устройства.

        По умолчанию параметр включен.

   e. Укажите учетную запись, под которой будет запущена задача *Проверка обновлений*. Вы можете использовать свою учетную запись и оставить включенным параметр **Учетная запись по умолчанию**. Кроме того, можно указать, что задача должна выполняться под другой учетной записью, имеющей необходимые права доступа. Для этого выберите параметр **Задать учетную запись** и введите учетные данные этой учетной записи.
6. Закройте окно свойств задачи *Загрузка обновлений в хранилище Сервера администрирования*, нажав на кнопку **Сохранить**.

Автоматическая проверка обновлений включена. Теперь вы можете запустить задачу *Загрузка обновлений в хранилище Сервера администрирования*, и она начнется с проверки обновлений.

Настройка точек распространения и шлюзов соединений

Структура групп администрирования в Kaspersky Security Center Linux 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.

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.

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.

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.

Если вы используете устройство под управлением Linux в качестве точки распространения, настоятельно рекомендуется увеличить ограничения дескрипторов файлов для службы klnagent, так как, если в область действия точки распространения входит много устройств, может не хватить максимального количества файлов, которые могут быть открыты по умолчанию.

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.

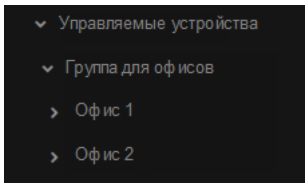
Возможны следующие способы построения структуры групп администрирования:

- 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.

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).



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.

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".

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

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:

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

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.

Автоматическое назначение точек распространения

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center Linux будет сам выбирать, какие устройства назначать точками распространения.

Чтобы назначить точки распространения автоматически:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Автоматически назначать точки распространения**.

   Если автоматическое назначение устройств точками распространения включено, невозможно вручную настраивать параметры точек распространения, а также изменять список точек распространения.

4. Нажмите на кнопку **Сохранить**.

В результате Сервер администрирования будет автоматически назначать точки распространения и настраивать их параметры.

Назначение точек распространения вручную

Развернуть все | Свернуть все

Kaspersky Security Center Linux позволяет вручную назначать устройства точками распространения.

Рекомендуется назначать точки распространения автоматически. В этом случае Kaspersky Security Center Linux 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.

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

Чтобы вручную назначить устройство точкой распространения:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Точки распространения**.

3. Выберите параметр **Вручную назначать точки распространения**.

4. Нажмите на кнопку **Назначить**.

5. Выберите устройство, которое вы хотите сделать точкой распространения.

   При выборе устройства учитывайте особенности работы точек распространения и требования к устройству, которое выполняет роль точки распространения.

6. Выберите группу администрирования, которую вы хотите включить в область действия выбранной точки распространения.

7. Нажмите на кнопку **ОК**.

   Добавленная точка распространения появится в списке точек распространения в разделе **Точки распространения**.

8. Нажмите на добавленную точку распространения в списке, чтобы открыть окно ее свойств.

9. В окне свойств настройте параметры точки распространения:

- В разделе **Общие** укажите параметры взаимодействия точки распространения с клиентскими устройствами.
  - **SSL-порт**

    Номер SSL-порта, по которому осуществляется защищенное подключение клиентских устройств к точке распространения с использованием протокола SSL.

    По умолчанию номер порта – 13000.

  - **Использовать многоадресную IP-рассылку**

    Если параметр включен, для автоматического распространения инсталляционных пакетов на клиентские устройства в пределах группы будет использоваться многоадресная IP-рассылка.

    Многоадресная IP-рассылка уменьшает время, необходимое для установки программ из инсталляционного пакета на группу клиентских устройств, но увеличивает время установки при установке программы на одно клиентское устройство.

  - **Адрес IP-рассылки**

    IP-адрес, на который будет выполняться многоадресная рассылка. IP-адрес можно задать в диапазоне 224.0.0.0 – 239.255.255.255

    По умолчанию Kaspersky Security Center Linux 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**

    IPv4-адрес, через который удаленные устройства подключаются к точке распространения.

  - **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 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 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**

  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 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.

- **Порт push-сервера**

  Номер порта push-сервера. Вы можете указать номер любого свободного порта.

- 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**

    Выберите источник обновлений для точки распространения:

    - Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.
    - Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*.
      - Если такая задача уже существует для устройства, выберите задачу в списке.
      - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

  - **Загрузить файлы различий**

    Этот параметр включает функцию загрузки файлов различий.

    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 **Шлюз соединения** можно настроить точку распространения как шлюз соединения для экземпляров Агента администрирования и Сервером администрирования:

  - **Шлюз соединения**

    Если прямое соединение между Сервером администрирования и Агентами администрирования не может быть установлено из-за организации вашей сети, вы можете использовать точку распространения в качестве шлюза соединения между Сервером администрирования и Агентами администрирования.

    Включите этот параметр, если требуется, чтобы точка распространения выполняла роль шлюза соединения между Агентами администрирования и Сервером администрирования. По умолчанию параметр выключен.

  - **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**

    Если Сервер администрирования находится за пределами демилитаризованной зоны (DMZ), в локальной сети, Агенты администрирования, установленные на удаленных устройствах, не могут подключаться к Серверу администрирования. Вы можете использовать точку распространения в качестве шлюза соединения с обратным подключением (Сервер администрирования устанавливает соединение с точкой распространения).

    Включите этот параметр, если требуется подключить Сервер администрирования к шлюзу соединения в демилитаризованной зоне.

  - **Открыть локальный порт для Kaspersky Security Center 14 Web Console**

    Включите этот параметр, если вам нужен шлюз соединения в демилитаризованной зоне, чтобы открыть порт для Web Console, находящейся в демилитаризованной зоне или в интернете. Укажите номер порта, который будет использоваться для подключения Web Console к точке распространения. По умолчанию установлен порт 13299.

    Это параметр доступен, если включен параметр **Установить соединение с шлюзом со стороны Сервера администрирования (если шлюз размещен в демилитаризованной зоне)**.

  При подключении мобильных устройств к Серверу администрирования через точку распространения, выполняющую роль шлюза соединения, вы можете включить следующие параметры:

  - **Открыть порт для мобильных устройств (SSL-аутентификация только Сервера администрирования)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт для мобильных устройств, и укажите номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13292. Мобильное устройство проверит сертификат Сервера администрирования. При установке соединения только Сервер администрирования выполняет аутентификацию.

  - **Открыть порт для мобильных устройств (двусторонняя SSL-аутентификация)**

    Включите этот параметр, если требуется, чтобы шлюз соединения открывал порт, который будет использоваться для двусторонней аутентификации Сервера администрирования и мобильных устройств. Мобильное устройство проверит сертификат Сервера администрирования, а Сервер администрирования проверит сертификат мобильного устройства. Задайте следующие параметры:

    - Номер порта, который мобильные устройства будут использовать для подключения к точке распространения. По умолчанию установлен порт 13293.
    - Имена DNS-доменов шлюза соединения, которые будут использоваться мобильными устройствами. Разделяйте имена доменов запятыми. Указанные имена доменов будут включены в сертификат точки распространения. Если имена доменов, используемые мобильными устройствами, не совпадают с общим именем в сертификате точки распространения, мобильные устройства не подключаются к точке распространения.

      Имя DNS-домена по умолчанию – это полное имя домена шлюза соединения.

В обоих случаях сертификаты проверяются во время установки TLS-сеанса только на точке распространения. Сертификаты не пересылаются на проверку Сервером администрирования. После установки TLS-сеанса с мобильным устройством точка распространения использует сертификат Сервера администрирования для создания туннеля для синхронизации между мобильным устройством и Сервером администрирования. Если вы откроете порт для двусторонней SSL-аутентификации, единственный способ распространить сертификат мобильного устройства – это с помощью установочного пакета.

- Настройте опрос IP-диапазонов точкой распространения.
  - **IP-диапазоны**;

    Вы можете включить обнаружение устройств для IPv4-диапазонов и IPv6-сетей.

    Если вы включили параметр **Разрешить опрос диапазона**, вы можете добавить диапазон опроса и задать расписание опроса. Вы можете добавить IP-диапазоны в список опрашиваемых диапазонов.

    Если включить параметр **Использовать Zeroconf для опроса IPv6-сетей**, точка распространения выполняет опрос IPv6-сети, используя сеть с нулевой конфигурацией (далее также *Zeroconf*). В этом случае указанные IP-диапазоны игнорируются, так как точка распространения опрашивает всю сеть. Параметр **Использовать Zeroconf для опроса IPv6-сетей** доступен, если точка распространения работает под управлением Linux. Чтобы использовать опрос Zeroconf IPv6, вы должны установить утилиту avahi-browse на точке распространения.

- В разделе **Дополнительно** укажите папку, которую точка распространения должна использовать для хранения распространяемых данных.
  - **Использовать папку по умолчанию**

    При выборе этого варианта для сохранения данных будет использоваться папка, в которую на точке распространения установлен Агент администрирования.

  - **Использовать указанную папку**

    При выборе этого варианта в расположенном ниже поле можно указать путь к папке. Папка может размещаться как локально на точке распространения, так и удаленно, на любом из устройств, входящих в состав сети организации.

    Учетная запись, под которой на точке распространения запускается Агент администрирования, должна иметь доступ к указанной папке для чтения и записи.

10. Нажмите на кнопку **OK**.

В результате выбранные устройства будут выполнять роль точек распространения.

Изменение списка точек распространения для группы администрирования

Вы можете просмотреть список точек распространения, назначенных для определенной группы администрирования, и изменить список, добавив или удалив точки распространения.

Чтобы просмотреть и изменить список точек распространения для группы администрирования:

1. В главном окне программы перейдите в раздел **Устройства → Управляемые устройства**.
2. В поле **Текущий путь** над списком управляемых устройств перейдите по ссылке.
3. В открывшейся панели слева выберите группу администрирования, для которой вы хотите просмотреть назначенные точки распространения.

   Для этого используйте пункт меню **Точки распространения**.
4. В главном окне программы перейдите в раздел **Устройства → Точки распространения**.
5. Чтобы добавить точки распространения для группы администрирования, нажмите на кнопку **Назначить**.
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 устройств с KasperskyOS с Сервером администрирования. Push-сервер имеет ту же область управляемых устройств, что и точка распространения, на которой включен push-сервер. Если у вас есть несколько точек распространения, назначенных для одной и той же группы администрирования, вы можете включить извещающий сервер на каждой них. В этом случае Сервер администрирования распределяет нагрузку между точками распространения.

Возможно, вы захотите использовать точки распространения в качестве push-серверов, чтобы обеспечить постоянную связь между управляемым устройством и Сервером администрирования. Постоянное соединение необходимо для некоторых операций, таких как запуск и остановка локальных задач, получение статистики для управляемой программы или создание туннеля. Если вы используете точку распространения в качестве сервера push-сервера, вам не нужно использовать параметр **Не разрывать соединение с Сервером администрирования** на управляемых устройствах или отправлять пакеты на UDP-порт Агента администрирования.

Push-сервер поддерживает нагрузку до 50 000 одновременных подключений.

Чтобы включить push-сервер на точке распространения:

1. Нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Точки распространения**.

3. Нажмите на имя точки распространения, на которой вы хотите включить push-сервер.

   Откроется окно свойств точки распространения.

4. В разделе **Общие** включите параметр **Запустить push-сервер**.

5. В поле **Порт push-сервера** укажите номер порта. Вы можете указать номер любого свободного порта.

6. В поле **Адрес удаленного устройства** укажите IP-адрес или имя точки распространения.

7. Нажмите на кнопку **ОК**.

Push-сервер включен на выбранной точке распространения.

Увеличение ограничения дескрипторов файлов для службы klnagent

Если область распространения точки распространения под управлением Linux включает в себя большое количество устройств, ограничения на количество открываемых файлов (дескрипторов файлов), которое было установлено по умолчанию, может быть недостаточно. Чтобы этого избежать, вы можете увеличить ограничение дескрипторов файлов для службы klnagent.

Чтобы увеличить ограничение дескрипторов файлов для службы klnagent

1. На устройстве под управлением Linux, которое выполняет роль точки распространения, откройте файл `/lib/systemd/system/klnagent64.service` и укажите жесткие и мягкие ограничения дескрипторов файлов в параметре `LimitNOFILE` раздела `[Service]`:

   `LimitNOFILE=< мягкое ограничение ресурсов >: жесткое ограничение ресурсов >`

   Например, `LimitNOFILE=32768:131072`. Обратите внимание, что мягкие ограничения дескрипторов файлов должны быть меньше или равны жесткому ограничению.

2. Выполните следующую команду, чтобы убедиться, что параметры указаны правильно:

   `systemd-analyze verify klnagent64.service`

   Если параметры указаны неверно, эта команда может вывести одну из следующих ошибок:

   - `/lib/systemd/system/klnagent64.service:11: Не удалось проанализировать значение ресурса, пропущено: 32768:13107`

     Если эта ошибка возникла, значит, символы в строке `LimitNOFILE` указаны неверно. Вам нужно проверить и исправить введенную строку.

   - `/lib/systemd/system/klnagent64.service:11: Мягкие ограничения ресурсов выбраны выше жесткого ограничения, пропущено: 32768:13107`

     Если эта ошибка возникла, мягкое ограничение введенных вами дескрипторов файлов превышает жесткое ограничение. Вам нужно проверить введенную строку и убедиться, что мягкое ограничение дескрипторов файлов меньше или равно жесткому ограничению.

3. Выполните следующую команду, чтобы перезагрузить процесс systemd:

   `systemctl daemon-reload`

4. Выполните следующую команду, чтобы перезапустить службу Агента администрирования:

   `systemctl restart klnagent`

5. Выполните следующую команду, чтобы убедиться, что указанные параметры применяются правильно:

   ```
   less /proc/<nagent_proc_id>/limits
   ```

   где параметр `<nagent_proc_id>` является идентификатором процесса Агента администрирования. Вы можете выполнить следующую команду, чтобы получить идентификатор:

   ```
   ps -ax | grep klnagent
   ```

Для точки распространения с операционной системой Linux количество открываемых файлов увеличено.

Создание задачи загрузки обновлений в хранилища точек распространения

Вы можете создать задачу *Загрузка обновлений в хранилища точек распространения* для группы администрирования. Такая задача будет выполняться для точек распространения, входящих в указанную группу администрирования.

Вы можете использовать эту задачу, например, если трафик между Сервером администрирования и точками распространения более дорогой, чем трафик между точками распространения и серверами обновлений "Лаборатории Касперского", или если у вашего Сервера администрирования нет доступа в интернет.

Эта задача необходима для загрузки обновлений с серверов обновлений "Лаборатории Касперского" в хранилища точек распространения. Список обновлений включает:

- обновления баз и программных модулей для программ безопасности "Лаборатории Касперского";
- обновления компонентов Kaspersky Security Center;
- обновления программ безопасности "Лаборатории Касперского".

После загрузки обновлений их можно распространять на управляемые устройства.

*Чтобы создать задачу **Загрузка обновлений в хранилища точек распространения** для выбранной группы администрирования:*

1. В главном окне программы перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.
3. Для программы Kaspersky Security Center выберите в поле **Task type** 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. На шаге **Завершение создания задачи**, если вы хотите изменить параметры задачи по умолчанию, включите параметр **Открыть окно свойств задачи после ее создания**. Если вы не включите этот параметр, задача будет создана с установленными по умолчанию значениями параметров. Установленные по умолчанию значения параметров можно изменить позже в любое время.
7. Нажмите на кнопку **Создать**.

   Задача будет создана и отобразится в списке задач.
8. Нажмите на имя созданной задачи, чтобы открыть окно свойств задачи.
9. На закладке **Параметры программы** окна свойств задачи укажите следующие параметры:

   - **Источники обновлений**

     В качестве источника обновлений для точек распространения могут быть использованы следующие ресурсы:

     - Серверы обновлений "Лаборатории Касперского"

       HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

       По умолчанию этот вариант выбран.
     - Главный Сервер администрирования

       Этот ресурс применяется к задачам, созданным для подчиненного или виртуального Сервера администрирования.
     - Локальная или сетевая папка

       Локальная или сетевая папка, которая содержит последние обновления. Сетевая папка может быть FTP-сервером, HTTP-сервером или общим ресурсом SMB. Если сетевая папка требует проверки подлинности, поддерживается только SMB-протокол. При выборе локальной папки требуется указать папку на устройстве с установленным Сервером администрирования.

FTP-сервер, HTTP-сервер или сетевая папка, используемые в качестве источника обновлений, должны содержать структуру папок (с обновлениями), которая соответствует структуре папок, созданной при использовании серверов обновлений "Лаборатории Касперского".

В задачах *Загружать обновления в хранилище Сервера администрирования* и *Загружать обновления в хранилища точек распространения* аутентификация пользователя не работает, если в качестве источника обновлений выбрана защищенная паролем локальная или сетевая папка. Чтобы решить эту проблему, сначала 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.

  По умолчанию параметр выключен.

- **Загружать обновления, используя старую схему**

  Начиная с версии 14, Kaspersky Security Center загружает обновления баз и программных модулей по новой схеме. Чтобы программа могла загружать обновления с помощью новой схемы, источник обновлений должен содержать файлы обновлений с метаданными, совместимыми с новой схемой. Если источник обновлений содержит файлы обновлений с метаданными, совместимыми только со старой схемой, включите параметр **Загружать обновления, используя старую схему**. Иначе задача загрузки обновлений завершится ошибкой.

  Например, этот параметр необходимо включить, если в качестве источника обновлений указана локальная или сетевая папка и файлы обновлений в этой папке были загружены одной из следующих программ:

  - Kaspersky Update Utility

    Эта утилита загружает обновления по старой схеме.

  - Kaspersky Security Center 13 Linux

    Например, точка распространения настроена на получение обновлений из локальной или сетевой папки. В этом случае вы можете загружать обновления с помощью Сервера администрирования, подключенного к интернету, а затем помещать обновления в локальную папку на точке распространения. Если Сервер администрирования имеет номер версии 13, включите параметр **Загружать обновления, используя старую схему** в задаче *Загружать обновления в хранилища точек распространения*.

  По умолчанию параметр выключен.

10. Создайте расписания запуска задачи. При необходимости настройте следующие параметры:

- **Запуск по расписанию**

  Выберите расписание, в соответствии с которым выполняется задача, и настройте выбранное расписание.

  - **Вручную** (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 программой, для которой вы создаете задачу.

  По умолчанию задача запускается каждый день, начиная с текущих системной даты и времени.

- **Каждую N неделю**

  Задача выполняется регулярно, с заданным интервалом в неделях, в указанный день недели и в указанное время.

  По умолчанию задача запускается каждую пятницу в текущее системное время.

- **Ежедневно (не поддерживается 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 Linux.

  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 программ, которые будут отслеживать вирусные атаки. Доступны следующие типы программ:

  - антивирусы для рабочих станций и файловых серверов;
  - антивирусы защиты периметра;
  - антивирусы для почтовых систем.

  По умолчанию выбраны все типы программ.

  Вы можете запускать разные задачи в зависимости от типа программы безопасности, сообщающей о вирусной атаке. В этом случае удалите выбор типов программ, которые вам не нужны.

- **По завершении другой задачи**

Текущая задача будет запущена после завершения другой задачи. Вы можете выбрать, как должна завершиться предыдущая задача (успешно или с ошибкой), чтобы запустить текущую задачу. Этот параметр работает, только если обе задачи назначены одним и тем же устройствам.

- **Запускать пропущенные задачи**

  Этот параметр определяет поведение задачи, если клиентское устройство не отображается в сети, когда задача вот-вот начнется.

  Если параметр включен, при очередном запуске программы "Лаборатории Касперского" на клиентском устройстве будет предпринята попытка запуска задачи. Если в расписании задачи указан запуск **Вручную**, **Один раз** или **Немедленно**, то задача запускается либо как только устройство становится видимым в сети, либо сразу после включения устройства в область действия задачи.

  Если параметр выключен, запуск задачи на клиентских устройствах будет производиться только по расписанию. 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 задачи**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени, то есть происходит *распределенный запуск задачи*. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Период распределенного запуска рассчитывается автоматически при создании задачи, в зависимости от количества клиентских устройств, которым назначена задача. Позже задача всегда запускается в расчетное время запуска. Однако когда в параметры задачи вносятся правки или задача запускается вручную, рассчитанное значение времени запуска задачи изменяется.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

- **Использовать случайную задержку запуска задачи в интервале (мин)**

  Если параметр включен, задача запускается на клиентских устройствах случайным образом в течение определенного интервала времени. Распределенный запуск задачи помогает избежать одновременного обращения большого количества клиентских устройств к Серверу администрирования при запуске задачи по расписанию.

  Если параметр выключен, запуск задачи на клиентских устройствах выполняется по расписанию.

  По умолчанию параметр выключен. По умолчанию интервал времени равен одной минуте.

11. 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.

Загрузка обновлений точками распространения

Развернуть все | Свернуть все

Kaspersky Security Center Linux 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 программы нажмите на значок настройки 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**

Выберите источник обновлений для точки распространения:

- Чтобы точка распространения получала обновления с Сервера администрирования, выберите вариант **Получить с Сервера администрирования**.
- Чтобы разрешить точке распространения получать обновления с помощью задачи, выберите **Использовать задачу загрузки обновлений в хранилище** и укажите задачу *Загружать обновления в хранилища точек распространения*:
  - Если такая задача уже существует для устройства, выберите задачу в списке.
  - Если такой задачи для устройства еще нет, перейдите по ссылке **Создать задачу** для создания задачи. Запустится мастер создания задачи. Следуйте далее указаниям мастера.

- **Загрузить файлы различий**

  Этот параметр включает функцию загрузки файлов различий.

  По умолчанию параметр включен.

В результате точка распространения будет получать обновления из указанного источника.

Добавление источников обновлений для задачи Загрузка обновлений в хранилище Сервера администрирования

При создании или использовании задачи загрузки обновлений в хранилище Сервера администрирования, 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".

Чтобы добавить источники обновлений:

1. Перейдите в раздел **Устройства** → **Задачи**.
2. Нажмите на кнопку **Загрузка обновлений в хранилище Сервера администрирования**.
3. Перейдите на закладку **Параметры программы**.
4. Около **Источники обновлений** нажмите на кнопку **Настроить**.
5. В появившемся окне нажмите на кнопку **Добавить**.
6. В списке источников обновлений добавьте необходимые источники. Если вы установите флажок **Локальная или сетевая папка**, укажите путь к папке.
7. Нажмите на кнопку **OK**, а затем закройте окно свойств источника обновлений.

8. В окне источника обновлений нажмите на кнопку **OK**.

9. Нажмите на кнопку **Сохранить** в окне задач.

Теперь обновления загружаются в хранилище Сервера администрирования из указанных источников.

Об использовании файлов различий для обновления баз и программных модулей "Лаборатории Касперского"

Когда Kaspersky Security Center Linux загружает обновления с серверов обновлений "Лаборатории Касперского", он оптимизирует трафик с помощью файлов различий. Вы также можете включить использование файлов различий устройствами (Серверов администрирования, точек распространения и клиентских устройств), которые принимают обновления с других устройств в вашей сети.

О функции загрузки файлов различий

Файл различий описывает различия между двумя версиями файлов базы или программного модуля. Использование файлов различий сохраняет трафик внутри сети вашей организации, так как файлы различий занимают меньше места, чем целые файлы баз и программных модулей. Если функция *Загрузить файлы различий* включена для Сервера администрирования или точки распространения, файлы различий сохраняются на этом Сервере администрирования или точке распространения. В результате устройства, которые получают обновления от этого Сервера администрирования или точки распространения, могут использовать сохраненные файлы различий для обновления своих баз и программных модулей.

Для оптимизации использования файлов различий рекомендуется синхронизировать расписание обновления устройств с расписанием обновлений Сервера администрирования или точки распространения, с которых это устройство получает обновления. Однако трафик может быть сохранен, даже если устройства обновляются в несколько раз реже, чем Сервер администрирования или точки распространения, с которых устройство получает обновления.

Точки распространения не используют многоадресную IP-рассылку для автоматического распространения файлов различий.

Включение функции загрузки файлов различий

Этапы

1. **Включение функции на Сервере администрирования**

   Включите функцию в свойствах задачи *Загрузка обновлений в хранилище Сервера администрирования*.

2. **Включение функции для точки распространения**

   Включить функцию для точки распространения, которая получает обновления с помощью задачи *Загрузка обновлений в хранилища точек распространения*.

   Включите функцию в параметрах политики Агента администрирования для точки распространения, которая получает обновления с Сервера администрирования.

   Включите функцию для точки распространения, которая получает обновления с Сервера администрирования.

   Эта функция включается в свойствах политики Агента администрирования и (если точки распространения назначены вручную и если вы хотите переопределить параметры политики) в свойствах Сервера администрирования в разделе **Точки распространения**.

Чтобы проверить, что функция загрузки файлов различий успешно включена, вы можете измерить внутренний трафик до и после выполнения сценария.

Обновление баз и программных модулей "Лаборатории Касперского" на автономных устройствах

Обновление баз и программных модулей "Лаборатории Касперского" на управляемых устройствах является важной задачей для обеспечения защиты устройств от вирусов и других угроз. Администратор обычно настраивает регулярное обновление с помощью хранилища Сервера администрирования.

Когда вам необходимо обновить базы данных и программные модули на устройстве (или группе устройств), которое не подключено к Серверу администрирования (главному или подчиненному), точке распространения или интернету, вам необходимо использовать альтернативные источники обновлений, такие как FTP-сервер или локальная папка. В этом случае вам нужно доставить файлы необходимых обновлений с помощью запоминающего устройства, такого как флеш-накопитель или внешний жесткий диск.

Вы можете скопировать требуемые обновления с:

- Сервера администрирования.

Чтобы хранилище Сервера администрирования содержало обновления, необходимые для программы безопасности, установленной на автономном устройстве, по крайней мере на одном из управляемых сетевых устройств должна быть установлена эта программа безопасности. Эта программа должна быть настроена на получение обновлений из хранилища Сервера администрирования с помощью задачи *Загрузка обновлений в хранилище Сервера администрирования*.

- Любого устройства, на котором установлена такая же программа безопасности и настроено получение обновлений из хранилища Сервера администрирования, хранилища точки распространения или напрямую с серверов обновлений "Лаборатории Касперского".

Ниже приведен пример настройки обновлений баз и программных модулей путем копирования их из хранилища Сервера администрирования.

Чтобы обновить базы данных и программные модули "Лаборатории Касперского" на автономных устройствах:

1. Подключите съемный диск к устройству, на котором установлен Сервер администрирования.
2. Скопируйте файлы обновлений на съемный диск.

   По умолчанию обновления расположены: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/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 для Linux на получение обновлений из локальной папки или общего ресурса, такого как FTP-сервер или общая папка.
4. Скопируйте файлы обновлений со съемного диска в локальную папку или общий ресурс, который вы хотите использовать в качестве источника обновлений.
5. На автономном устройстве, на которое требуется установить обновления, запустите задачу обновления Kaspersky Endpoint Security для Linux.

После завершения задачи обновления базы данных и программные модули "Лаборатории Касперского" будут обновлены на устройстве.

Резервное копирование и восстановление веб-плагинов

Kaspersky Security Center 14 Web Console позволяет создавать резервную копию данных текущего состояния веб-плагина, чтобы впоследствии можно было восстановить сохраненное состояние. Например, вы можете создать резервную копию данных веб-плагина перед его обновлением до более новой версии. После обновления, если более новая версия не соответствует вашим требованиям или ожиданиям, вы можете восстановить предыдущую версию веб-плагина из резервной копии данных.

Для резервного копирования данных веб-плагинов:

1. В главном окне программы перейдите в раздел **Параметры → Веб-плагины**.
2. В разделе **Веб-плагины** выберите веб-плагины, для которых требуется создать резервную копию данных и нажмите на кнопку **Создать резервную копию данных**.

Резервное копирование данных выбранных веб-плагинов. Вы можете просмотреть созданные резервные копии данных на вкладке **Резервные копии данных**.

Чтобы восстановить веб-плагин из резервной копии данных:

1. В главном окне программы перейдите в раздел **Параметры → Резервные копии данных**.
2. В разделе **Резервные копии данных** выберите резервную копию данных веб-плагина, который вы хотите восстановить, а затем нажмите на кнопку **Восстановить из резервной копии данных**.

Веб-плагин восстанавливается из выбранной резервной копии данных.

Управление сторонними программами и исполняемыми файлами на клиентских устройствах

В этом разделе описаны возможности Kaspersky Security Center Linux связанные с управлением сторонних программ и исполняемых файлов на клиентских устройствах.

Сценарий: Управление программами

Вы можете управлять запуском программ на пользовательских устройствах. Вы можете разрешить или запретить запуск программ на управляемых устройствах. Эта функциональность реализуется компонентом Контроль программ.

Компонент Контроль программ доступен для версии программы Kaspersky Endpoint Security 11.2 для Linux и выше.

Предварительные требования

- Kaspersky Security Center Linux развернут в вашей организации.
- Политика Kaspersky Endpoint Security для Linux создана и активна.

Этапы

Сценарий использования компонента Контроль программ состоит из следующих этапов:

1. **Формирование и просмотр списка исполняемых файлов на клиентских устройствах**

   Этот этап помогает вам определить, какие исполняемые файлы обнаружены на управляемых устройствах. Просмотрите список исполняемых файлов и сравните его со списками разрешенных и запрещенных исполняемых файлов. Ограничения использования исполняемых файлов могут быть связаны с политиками информационной безопасности в вашей организации. Вы можете пропустить этот этап, если точно знаете, какие исполняемые файлы установлены на управляемых устройствах.

   Инструкции: Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах.

2. **Создание категорий программ для программ, используемых в вашей организации**

   Проанализируйте списки исполняемых файлов, хранящихся на управляемых устройствах. На основании анализа создайте категории программ. Рекомендуется создать категорию "Рабочие программы", которая охватывает стандартный набор программ, используемых в вашей организации. Если разные группы безопасности используют разные наборы программ в своей работе, для каждой группы безопасности можно создать отдельную категорию программ.

   Инструкции: Создание пополняемой вручную категории программ.

3. **Настройка компонента Контроль программ в политике Kaspersky Endpoint Security для Linux**

   Настройте компонент Контроль программ в политике Kaspersky Endpoint Security для Linux с использованием категорий программ, которые вы создали на предыдущем этапе.

4. **Проверка конфигурации Контроля программ**

   Убедитесь, что вы выполнили следующее:

   - Создали категории программ.
   - Настроили Контроль программ с использованием категорий программ.

Результаты

После завершения сценария, запуск программ на управляемых устройствах контролируется. Пользователи могут запускать только те программы, которые разрешены в вашей организации, и не могут запускать программы, запрещенные в вашей организации.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux.

О Контроле программ

Компонент Контроль программ контролирует попытки пользователей запуска программ и регулирует запуск программ с помощью правил Контроля программ.

> Компонент Контроль программ доступен для версии программы Kaspersky Endpoint Security 11.2 для Linux и выше.

Запуск программ, параметры которых не соответствуют ни одному из правил Контроля программ, регулируется выбранным режимом работы компонента:

- *Список запрещенных*. Режим используется, если вы хотите разрешить запуск всех программ, кроме программ, указанных в запрещающих правилах. По умолчанию выбран этот режим.
- *Список разрешенных*. Режим используется, если вы хотите заблокировать запуск всех программ, кроме программ, указанных в разрешающих правилах.

Правила Контроля программ реализуются с помощью категорий программ. Вы создаете категории программ с определенными критериями. В Kaspersky Security Center Linux можно создавать только пользовательские категории программ, пополняемые вручную. Вы определяете условия, например, метаданные файла, хеш файла, сертификат файла, KL-категория, путь к файлу, чтобы включить исполняемые файлы в категорию.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux.

Получение и просмотр списка исполняемых файлов, хранящихся на клиентских устройствах

Вы можете получить список исполняемых файлов, хранящихся на управляемых устройствах. Для инвентаризации исполняемых файлов вы должны создать задачу инвентаризации.

Функция инвентаризации исполняемых файлов доступна для версии программы Kaspersky Endpoint Security 11.2 для Linux и выше.

Чтобы создать задачу инвентаризации исполняемых файлов на клиентских устройствах:

1. Перейдите в раздел **Устройства** → **Задачи**.

   Отобразится список задач.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания задачи. Следуйте далее указаниям мастера.

3. На странице **Новая задача** из раскрывающегося списка **Программа** выберите Kaspersky Endpoint Security для Linux.

4. В раскрывающемся списке **Тип задачи** выберите **Инвентаризация**.

5. На странице **Завершение создания задачи** нажмите на кнопку **Готово**.

   После того как мастер создания задачи завершит свою работу, задача **Инвентаризация** создана и настроена. Вы можете изменить параметры созданной задачи. В результате созданная задача отобразится в списке задач.

Подробное описание задачи инвентаризации см. в онлайн-справке Kaspersky Endpoint Security для Linux.

После выполнения задачи **Инвентаризация** формируется список исполняемых файлов, хранящихся на управляемых устройствах, и вы можете просмотреть этот список.

При выполнении инвентаризации программа обнаруживает исполняемые файлы следующих форматов: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR и HTML-файлы.

Чтобы просмотреть список исполняемых файлов, хранящихся на клиентских устройствах,

В раскрывающемся списке **Операции** → **Программы сторонних производителей** выберите **Исполняемые файлы**.

На странице отобразится список исполняемых файлов, хранящихся на клиентских устройствах.

Создание пополняемой вручную категории программ

Развернуть все | Свернуть все

Вы можете указать набор критериев в качестве шаблона для исполняемых файлов, запуск которых вы хотите разрешить или запретить в своей организации. На основе исполняемых файлов, соответствующих критериям, вы можете создать категорию программ и использовать ее в настройке компонента Контроль программ.

Чтобы создать пополняемую вручную категорию программ:

1. В раскрывающемся списке **Операции** → **Программы сторонних производителей** выберите **Категории программ**.

   Откроется страница со списком категорий программ.

2. Нажмите на кнопку **Добавить**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. На шаге **Выбор способа создания категории** 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:

   - **Выберите сертификат из хранилища сертификатов**

     Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

   - **Задайте путь к программе (поддерживаются маски)**

Если выбран этот вариант, можно указать папку на клиентском устройстве, исполняемые файлы из которой будут добавлены в пользовательскую категорию программ.

- Съемный диск

  Если выбран этот вариант, можно указать тип носителя (любой или съемный диск), на котором выполняется запуск программы. Программы, запускаемые на носителе выбранного типа, будут добавлены в пользовательскую категорию программ.

- **Хеши файлов папки, метаданные файлов папки или сертификаты из папки**:

  - Выберите из списка исполняемых файлов

    Если выбран этот вариант, программы для добавления в категорию можно выбрать из списка исполняемых файлов на клиентском устройстве.

  - Выберите из реестра программ

    Если выбран этот параметр, отображается реестр программ. Вы можете выбрать программы из реестра и указать следующие метаданные файла:

    - Имя файла.
    - Версия файла. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Название программы.
    - Версия программы. Вы можете указать точное значение версии или написать условие, например, "больше, чем 5.0".
    - Производитель.

  - Задайте вручную

    Если выбран этот вариант, вы должны указать хеш файла, метаданные или сертификат в качестве условия добавления программ в пользовательскую категорию.

    Хеш файла

    В зависимости от версии программы безопасности, установленной на устройствах в вашей сети, необходимо выбрать алгоритм вычисления хеш-функции программой Kaspersky Security Center Linux 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 программой Kaspersky Security Center Linux для файлов категории:

    - Если все экземпляры программ безопасности, установленных в вашей сети, являются Kaspersky Endpoint Security для Linux, установите флажок **SHA-256**.
    - Установите флажок **MD5-хеш**, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

    Метаданные

    Если этот параметр выбран, вы можете указать метаданные файла такие как имя файла, версию файла и поставщика. Метаданные будут передаваться на Сервер администрирования. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в категорию программ.

    Сертификат

    Если выбран этот вариант, можно указать сертификаты из хранилища. Исполняемые файлы, подписанные в соответствии с указанными сертификатами, будут добавлены в пользовательскую категорию.

  - Из архивной папки

    Если выбран этот параметр, вы можете указать файл в архивной папке и выбрать, какое условие вы хотите использовать для добавления программ в пользовательскую категорию. Архивная папка распаковывается, и выбранные условия применяются к файлам в этой папке. В качестве условия, можно выбрать один следующих критериев:

    - **Хеш файла**

Вы можете выбрать, какую хеш-функцию (MD5 или SHA256) вы хотите использовать для вычисления значения хеш-функции. Программы, имеющие такой же хеш, как и файлы в архивной папке, будут добавлены в пользовательскую категорию программ.

Выберите хеш-функцию MD5, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

- **Метаданные**

  Выберите, какие метаданные вы хотите использовать в качестве критерия. Исполняемые файлы, имеющие такие же метаданные, будут добавлены в пользовательскую категорию программ.

- **Сертификат**

  Выберите, какие параметры сертификата (имя субъекта сертификата, отпечаток пальца или кем выписан сертификат) вы хотите использовать в качестве критерия. Исполняемые файлы, подписанные сертификатами, которые имеют те же параметры, будут добавлены в пользовательскую категорию.

Выбранный критерий добавлен в список условий.

Вы можете добавить столько критериев для создания категории программ, сколько вам нужно.

6. На шаге **Исключения** нажмите на кнопку **Добавить**, чтобы добавить критерий в область исключений и исключить файлы из создаваемой категории.

7. На шаге **Критерии условия**, выберите тип правила из списка, так же, как вы выбрали тип правила для создания категории.

После завершения мастера создается категория программ. Оно появится в списке категорий программ. Вы можете создать категорию программ при настройке компонента Контроль программ.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux.

Просмотр списка категорий программ

Вы можете просмотреть список настроенных категорий программ и параметры каждой категории программ.

Чтобы просмотреть список категорий программ,

На закладке **Операции** в раскрывающемся списке **Программы сторонних производителей** выберите **Категории программ**.

Откроется страница со списком категорий программ.

Чтобы просмотреть свойства категории программ,

нажмите на имя категории программ.

Откроется окно свойств выбранной категории программ. Параметры сгруппированы на нескольких закладках.

Добавление исполняемых файлов, связанных с событием, в категорию программы

После настройки компонента Контроль программ в политиках Kaspersky Endpoint Security для Linux в списке событий могут отображаться следующие события:

- **Запуск программы запрещен** (*Критическое* событие). Это событие отображается, если вы настроили Контроль программ для применения правил.
- **Запуск программы запрещен в тестовом режиме** (*Информационное* событие). Это событие отображается, если вы настроили Контроль программ для применения правил в тестовом режиме.
- **Сообщение администратору о запрете запуска программы** (сообщение с уровнем важности *Предупреждение*). Это событие отображается, если вы настроили Контроль программ для применения правил, а пользователь запросил доступ к программе, которая заблокирована для запуска.

Рекомендуется создавать выборки событий для просмотра событий, связанных с компонентом Контроль программ.

Вы можете добавить исполняемые файлы, связанные с событиями Контроля программ, в существующую категорию программ или в новую категорию программ. Вы можете добавлять исполняемые файлы только в категорию программ пополняемую вручную.

Чтобы добавить исполняемые файлы, связанные с событиями компонента Контроль программ, в категорию программ:

1. Перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.

Отобразится список выборок событий.

2. Выберите выборку событий, чтобы просмотреть события, связанные с Контролем программ, и запустите формирование этой выборки событий.

   Если вы не создали выборку событий, связанную с Контролем программ, вы можете выбрать и запустить предопределенную выборку, например, **Последние события**.

   Отобразится список событий.

3. Выберите события, связанные исполняемые файлы которых, вы хотите добавить в категорию программ, и нажмите на кнопку **Назначить категорию**.

   Запустится мастер создания категории. Для продолжения работы мастера нажмите на кнопку **Далее**.

4. На странице мастера укажите необходимые параметры:

   - В разделе **Действие с исполняемым файлом, связанным с событием** выберите один из следующих вариантов:

     - **Добавить в новую категорию программ**

       Выберите этот параметр, если вы хотите создать категорию программ на основе исполняемых файлов, связанных с событиями.

       По умолчанию выбран этот вариант.

       Если вы выбрали этот параметр, укажите имя новой категории.

     - **Добавить в существующую категорию**

       Выберите этот параметр, если вы хотите добавить исполняемые файлы, связанные с событиями, в существующую категорию программ.

       По умолчанию вариант не выбран.

       Если вы выбрали этот параметр, выберите категорию программ, пополняемую вручную, в которую вы хотите добавить исполняемые файлы.

   - В разделе **Тип правила** выберите один из следующих вариантов:

     - **Правила для добавления в область действия**
     - **Правила для добавления в исключения**

   - В разделе **Параметр, используемый в качестве условия** выберите один из следующих вариантов:

     - **Данные сертификата (или SHA-256 для файлов без сертификата)**

       Файлы могут быть подписаны сертификатом. При этом одним сертификатом могут быть подписаны несколько файлов. Например, разные версии одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

       Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

       Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла или хеш-функцию 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 одной программы могут быть подписаны одним сертификатом или несколько разных программ одного производителя могут быть подписаны одним сертификатом. При выборе сертификата в категорию может попасть несколько версий программы или несколько программ одного производителя.

       Выберите этот вариант, если в правила категории необходимо добавить данные сертификата исполняемого файла. Если у исполняемого файла нет сертификата, то такой файл будет пропущен. Информация о нем не будет добавлена в категорию.

     - **Только SHA-256 (файлы без хеша пропускаются)**

       Каждый файл имеет свою уникальную хеш-функцию SHA256. При выборе хеш-функции SHA256 в категорию попадает только один соответствующий файл, например, заданная версия программы.

       Выберите этот вариант, если в правила категории необходимо добавить только данные хеш-функции SHA256 исполняемого файла.

- **Только MD5 (для совместимости с Kaspersky Endpoint Security 10 Service Pack 1)**

  Выберите этот параметр, только если вы используете Kaspersky Endpoint Security для Windows. Kaspersky Endpoint Security для Linux не поддерживает хеш-функцию MD5.

  Каждый файл имеет свою уникальную хеш-функцию MD5. При выборе хеш-функции MD5 в категорию попадает только один соответствующий файл, например, заданная версия программы.

5. Нажмите на кнопку **OK**.

После завершения работы мастера исполняемые файлы, связанные с событиями Контроля программ, добавляются в существующую категорию программ или в новую категорию программ. Вы можете просмотреть параметры категории программ, которую вы изменили или создали.

Подробнее о Контроле программ см. в справке Kaspersky Endpoint Security для Linux.

Мониторинг и отчеты

В этом разделе описаны функции мониторинга и работа с отчетами в Kaspersky Security Center Linux. Эти функции позволяют получать сведения об инфраструктуре вашей сети, статусе защиты, а также статистику.

В процессе развертывания или во время работы Kaspersky Security Center Linux можно настраивать функции мониторинга и параметры отчетов.

Сценарий: Мониторинг и отчеты

В этом разделе представлен сценарий настройки мониторинга и отчетов в Kaspersky Security Center Linux.

Предварительные требования

После развертывания Kaspersky Security Center Linux 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, 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.

3. **Выполнение рекомендуемых действий для критических и предупреждающих уведомлений**

   Инструкции:

   Выполните рекомендуемые действия для сети вашей организации.

4. **Просмотр состояния безопасности сети вашей организации**

   Инструкции:

   - Просмотр веб-виджета Состояние защиты.
   - Генерация и просмотр отчета Отчет о состоянии защиты.
   - Генерация и просмотр отчета Отчет об ошибках.

5. **Нахождение незащищенных клиентских устройств**

Инструкции:

- Просмотр веб-виджета Новые устройства.
- Генерация и просмотр отчета Отчет о развертывании защиты.

6. **Проверка защиты клиентских устройств**

   Инструкции:

   - Генерация и просмотр отчета из категорий Состояние защиты и Статистика угроз.
   - Запуск и просмотр выборки событий Критическое.

7. **Оценка и ограничение загрузки событий в базу данных**

   Информация о событиях, которые возникают во время работы управляемых программ, передается с клиентского устройства и регистрируется в базе данных Сервера администрирования. Чтобы снизить нагрузку на Сервер администрирования, оцените и ограничьте максимальное количество событий, которые могут храниться в базе данных.

   Инструкции:

   - Ограничение максимального количества событий.

8. **Просмотр информации о лицензии**

   Инструкции:

   - Добавление веб-виджета Используемые лицензионные ключи на панель мониторинга и его просмотр.
   - Генерация и просмотр отчета Отчет об использовании лицензионных ключей.

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 14 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**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 14 Web Console.

Уведомления

Уведомления предназначены для оповещения о событиях и для того, чтобы помочь вам увеличить скорость ваших ответов на эти события, выполнив рекомендуемые действия, которые вы считаете подходящими.

Панель мониторинга и веб-виджеты

В этом разделе содержится информация о панели мониторинга и веб-виджетах, представленных на панели мониторинга. Раздел содержит инструкции по управлению веб-виджетами и настройке веб-виджетов.

Использование панели мониторинга

Панель мониторинга позволяет контролировать состояние безопасности в сети вашей организации с помощью графического представления информации.

Панель мониторинга доступна в Kaspersky Security Center 14 Web Console в разделе **Мониторинг и отчеты → Панель мониторинга**.

На панели мониторинга представлены настраиваемые веб-виджеты. Вы можете выбрать большое количество различных веб-виджетов, представленных в виде круговых диаграмм, таблиц, графиков, гистограмм и списков. Информация, отображаемая в веб-виджетах, обновляется автоматически, период обновления составляет от одной до двух минут. Интервал времени между обновлениями зависит от типа веб-виджета. Вы можете обновить данные веб-виджета вручную с помощью меню, в любое время.

По умолчанию веб-виджеты включают информацию о событиях, хранящихся в базе данных Сервера администрирования.

Kaspersky Security Center 14 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, скрывать веб-виджеты, а также менять внешний вид или размер веб-виджетов, перемещать веб-виджеты и изменять параметры веб-виджетов.

Добавление веб-виджета на информационную панель

Чтобы добавить веб-виджет на информационную панель:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на кнопку **Добавить или восстановить веб-виджет**.
3. В списке доступных веб-виджетов выберите веб-виджет, который требуется добавить на информационную панель.

   Веб-виджеты сгруппированы по категориям. Чтобы посмотреть, какие веб-виджеты входят в категорию, нажмите на значок шеврона (›) рядом с именем категории.
4. Нажмите на кнопку **Добавить**.

Выбранные веб-виджеты будут добавлены в конец информационной панели.

Можно изменить внешний вид и параметры добавленных веб-виджетов.

Удаление веб-виджета с информационной панели

Чтобы удалить веб-виджет с информационной панели:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Панель мониторинга**.
2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется удалить.

3. Выберите **Скрыть веб-виджет**.

4. В появившемся окне **Предупреждение** нажмите на кнопку **ОК**.

Выбранный веб-виджет будет удален с информационной панели. В дальнейшем можно опять добавить веб-виджет на информационную панель.

Перемещение веб-виджета на информационной панели

Чтобы переместить веб-виджет на информационной панели:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется переместить.

3. Выберите **Переместить**.

4. Укажите место, куда требуется переместить веб-виджет. Можно выбрать только другой веб-виджет.

Выбранные веб-виджеты поменяются местами.

Изменение размера или внешнего вида виджета

Можно изменить внешний вид веб-виджетов: выбрать столбчатую или линейную диаграмму. Для некоторых веб-виджетов можно изменить размер: маленький, средний или крупный.

Чтобы изменить внешний вид веб-виджета:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.

3. Выполните одно из следующих действий:

   - Чтобы веб-виджет отображался как столбчатая диаграмма, выберите **Тип диаграммы: линейчатая диаграмма**.
   - Чтобы веб-виджет отображался как линейная диаграмма, выберите **Тип диаграммы: линейный график**.
   - Чтобы поменять размер области, занимаемой веб-виджетом, выберите одно из значений:
     - **Минимальный**
     - **Минимальный (только линейчатая диаграмма)**
     - **Средний (кольцевой график)**
     - **Средний (линейчатая диаграмма)**
     - **Максимальный**

Внешний вид выбранного веб-виджета будет изменен.

Изменение параметров веб-виджета

Чтобы изменить параметры веб-виджета:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Панель мониторинга**.

2. Нажмите на значок параметров (⚙) рядом с веб-виджетом, который требуется изменить.

3. Выберите **Показать параметры**.

4. В открывшемся окне параметров веб-виджета измените требуемые параметры веб-виджета.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Параметры выбранного веб-виджета будут изменены.

Набор параметров зависит от конкретного веб-виджета. Ниже приведены некоторые общие параметры:

- **Область веб-виджета** – набор объектов, для которых веб-виджет отображает информацию; например, группа администрирования или выборка устройств.
- **Выберите задачу** – 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", если** и **Установить статус "Предупреждение", если** – 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 программы 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.

О режиме Просмотра только панели мониторинга

Вы можете настраивать режим Просмотра только панели мониторинга для сотрудников, которые не управляют сетью, но хотят просматривать статистику защиты сети в Kaspersky Security Center (например, это может быть топ-менеджер). Когда у пользователя включен этот режим, у пользователя отображается только панель мониторинга с предопределенным набором веб-виджетов. Таким образом, пользователь может просматривать указанную в веб-виджетах статистику, например, состояние защиты всех управляемых устройств, количество недавно обнаруженных угроз или список наиболее частых угроз в сети.

При работе пользователя в режиме Просмотра только панели мониторинга применяются следующие ограничения:

- Главное меню не отображается, поэтому пользователь не может изменить параметры защиты сети.
- Пользователь не может выполнять действия с веб-виджетами, например, добавлять или скрывать их. Поэтому нужно разместить на панели мониторинга все необходимые пользователю веб-виджеты и настроить их, например, задать правило подсчета объектов или указать период.

Вы не можете назначить режим Просмотра только панели мониторинга себе. Если вы хотите работать в этом режиме, обратитесь к системному администратору, поставщику услуг (MSP) или пользователю с правами **Изменение списков управления доступом объектов** в функциональной области **Общие функции: Права пользователя**.

Настройка режима Просмотра только панели мониторинга

Перед началом настройки режима Просмотра только панели мониторинга убедитесь, что выполнены следующие предварительные требования:

- У вас есть право **Modify object ACLs** в функциональной области **Общие функции: Права пользователя**. Если у вас нет этого права, закладка для настройки режима будет отсутствовать.
- Пользователь с правом **Чтение** 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 в разделе **Пользователи и роли → Пользователи**. Это может быть главный Сервер или физический подчиненный Сервер. На виртуальном Сервере администрирования настроить режим Просмотра только панели мониторинга нельзя.

Чтобы настроить режим Просмотра только панели мониторинга:

1. В главном окне программы перейдите в раздел **Пользователи и роли → Пользователи**.
2. Нажмите на имя учетной записи пользователя, для которой вы хотите настроить панель инструментов с веб-виджетами.
3. В открывшемся окне свойств учетной записи выберите закладку **Панель мониторинга**.

   На открывшейся закладке отображается та же панель мониторинга, что и для пользователя.
4. Если параметр **Отображать режим Просмотра только панели мониторинга** включен, выключите его переключателем.

   Когда этот параметр включен, также нельзя изменить панель мониторинга. После выключения параметра можно управлять веб-виджетами.
5. Настройте внешний вид панели мониторинга. Набор веб-виджетов, подготовленный на закладке **Панель мониторинга**, доступен для пользователя с настраиваемой учетной записью. Пользователь с такой учетной записью не может изменять какие-либо параметры или размер веб-виджетов, добавлять или удалять веб-виджеты с панели мониторинга. Поэтому настройте их под пользователя, чтобы он мог

просматривать статистику защиты сети. С этой целью на закладке **Панель мониторинга** можно выполнять те же действия с веб-виджетами, что и в разделе **Мониторинг и отчеты → Панель мониторинга**:

- Добавлять веб-виджеты на панель мониторинга.
- Скрывать веб-виджеты, которые не нужны пользователю.
- Перемещать веб-виджеты в определенном порядке.
- Изменять размер или внешний вид веб-виджетов.
- Изменять параметры веб-виджетов.

6. Переключите переключатель, чтобы включить параметр **Отображать режим Просмотра только панели мониторинга**.

   После этого пользователю доступна только панель мониторинга. Пользователь может просматривать статистику, но не может изменять параметры защиты сети и внешний вид панели мониторинга. Так как вам отображается та же панель мониторинга, что и для пользователя, вы также не можете изменить панель мониторинга.

   Если оставить этот параметр выключенным, у пользователя отображается главное меню, поэтому он может выполнять различные действия в Kaspersky Security Center, в том числе изменять параметры безопасности и веб-виджеты.

7. Нажмите на кнопку **Сохранить**, когда закончите настройку режима Просмотра только панели мониторинга. Только после этого подготовленная панель мониторинга будет отображаться у пользователя.

8. Если пользователь хочет просмотреть статистику поддерживаемых программ "Лаборатории Касперского" и ему нужны для этого права доступа, настройте права для этого пользователя. После этого данные программ "Лаборатории Касперского" отображаются у пользователя в веб-виджетах этих программ.

Теперь пользователь может входить в Kaspersky Security Center под настраиваемой учетной записью и просматривать статистику защиты сети в режиме Просмотра только панели мониторинга.

Отчеты

В этом разделе описывается, как использовать отчеты, управлять шаблонами пользовательских отчетов, использовать шаблоны для создания отчетов и создавать задачи рассылки отчетов.

Использование отчетов

Отчеты позволяют вам получить подробную числовую информацию о безопасности сети вашей организации для сохранения этой информации в файл, отправки ее по электронной почте и печати.

Отчеты доступны в Kaspersky Security Center 14 Web Console в разделе **Мониторинг и отчеты → Отчеты**.

По умолчанию отчеты включают информацию за последние 30 дней.

Kaspersky Security Center Linux имеет по умолчанию набор отчетов для следующих категорий:

- **Состояние защиты**
- **Развертывание**
- **Обновление**
- **Статистика угроз**
- **Другие**

Вы можете создавать пользовательские шаблоны отчетов, редактировать шаблоны отчетов и удалять их.

Можно создавать отчеты на основе существующих шаблонов, экспортировать отчеты в файл и создавать задачи рассылки отчетов.

Создание шаблона отчета

Чтобы создать шаблон отчета:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Нажмите на кнопку **Добавить**.

   В результате запустится мастер создания шаблона отчета. Для продолжения работы мастера нажмите на кнопку **Далее**.

3. Введите название отчета и выберите тип отчета.

4. На шаге мастера **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 мастера **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.

Просмотр и изменение свойств шаблона отчета

Развернуть все | Свернуть все

Вы можете просматривать и изменять основные свойства шаблона отчета, например, имя шаблона отчета или поля, отображаемые в отчете.

Чтобы просмотреть и изменить свойства шаблона отчета:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.

2. Установите флажок напротив шаблона отчета, свойства которого вы хотите просмотреть и изменить.
   В качестве альтернативы можно сначала сформировать отчет, а затем нажать на кнопку **Изменить**.

3. Нажмите на кнопку **Открыть свойства шаблона отчета**.
   Откроется окно **Изменение отчета <имя отчета>** на закладке **Общие**.

4. Измените свойства шаблона отчета:

   - Закладка **Общие**:
     - Название шаблона отчета
     - **Максимальное число отображаемых записей**

       Если этот параметр включен, количество отображаемых в таблице записей с подробными данными отчета не превышает указанное значение.

       Записи отчета сначала сортируются в соответствии с правилами, указанными в разделе **Графы → Детальные данные** свойств шаблона отчета, а затем сохраняется только первая часть результирующих записей. В заголовке таблицы с подробными данными отчета показано отображаемое количество записей и общее количество записей, соответствующее другим параметрам шаблона отчета.

       Если этот параметр выключен, в таблице с подробными данными отчета отображаются все записи. Не рекомендуется выключать этот параметр. Ограничение количества отображаемых записей отчета снижает нагрузку на систему управления базами данных и время, требуемое для формирования и экспорта отчета. В некоторых отчетах содержится слишком большое количество записей. В таких случаях просмотр и анализ всех записей может оказаться слишком трудоемким. Также на устройстве при формировании такого отчета может закончиться память. Это может привести к тому, что вам не удастся просмотреть отчет.

       По умолчанию параметр включен. По умолчанию указано значение 1000.

     - **Группа**

       Нажмите на кнопку **Параметры**, чтобы изменить набор клиентских устройств, для которых создается отчет. Для некоторых типов отчетов кнопка может быть недоступна. Реальные данные зависят от значений параметров, указанных при создании шаблона отчета.

     - **Период**

       Нажмите на кнопку **Параметры**, чтобы изменить период, за который будет сформирован отчет. Для некоторых типов отчетов кнопка может быть недоступна. Доступные значения:

- между двумя указанными датами;
- от указанной даты до даты создания отчета;
- от даты создания отчета минус указанное количество дней до даты создания отчета.

- **Включать данные подчиненных и виртуальных Серверов администрирования**

  Если этот параметр включен, отчет содержит информацию с подчиненных и виртуальных Серверов администрирования, которые подчинены Серверу администрирования, для которого создан шаблон отчета.

  Выключите этот параметр, если вы хотите просматривать данные только текущего Сервера администрирования.

  По умолчанию параметр включен.

- **До уровня вложенности**

  Отчет содержит данные подчиненных и виртуальных Серверов администрирования, которые находятся под текущим Сервером администрирования на уровне вложенности ниже или равном указанному значению.

  По умолчанию указано значение 1. Вы можете изменить это значение, если вы хотите видеть в отчете информацию подчиненных Серверов администрирования, расположенных на более низких уровнях вложенности дерева.

- **Интервал ожидания данных (мин)**

  Сервер администрирования, для которого создан шаблон отчета, ожидает данные от подчиненных Серверов администрирования в течение указанного времени для создания отчета. Если данные не получены от подчиненного Сервера администрирования в течение указанного интервала времени, отчет запускается в любом случае. Вместо фактических данных в отчете отображаются данные, полученные из кеша (если включен параметр **Кешировать данные с подчиненных Серверов администрирования**), или в противном случае **N/A** (Недоступно).

  По умолчанию время ожидания составляет 5 минут.

- **Кешировать данные с подчиненных Серверов администрирования**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Переданные данные хранятся в кеше.

  Если Сервер администрирования не может получить данные подчиненного Сервера администрирования во время генерации отчета, в отчете отобразятся данные из кеша. В этом случае отображается дата, когда данные были переданы в кеш.

  Включение этой опции позволяет просматривать информацию, полученную от подчиненных Серверов администрирования, даже если невозможно получить актуальные данные. Однако отображаемые данные могут быть устаревшими.

  По умолчанию параметр выключен.

- **Период обновления данных в кеше (ч)**

  Подчиненные Серверы администрирования регулярно передают данные на главный Сервер администрирования, для которого создан шаблон отчета. Вы можете указать этот период в часах. Если установлено значение 0, данные передаются только во время генерации отчета.

  По умолчанию указано значение 0.

- **Передавать подробную информацию с подчиненных Серверов администрирования**

  В созданном отчете таблица с подробными данными включает информацию с подчиненных Серверов администрирования главного Сервера администрирования, для которого создан шаблон отчета.

  Если этот параметр включен, то замедляется создание отчета и увеличивается трафик между Серверами администрирования. Однако вы можете просмотреть все данные в одном отчете.

  Чтобы не включать этот параметр, вы можете проанализировать данные отчета для нахождения неисправного подчиненного Сервера администрирования, а затем сформировать этот же отчет только для него.

  По умолчанию параметр выключен.

- Закладка **Графы**

  Выберите поля, которые будут отображаться в отчете. С помощью кнопок **Вверх** и **Вниз** измените порядок отображения полей. С помощью кнопок **Добавить** и **Изменить** укажите, будет ли информация в отчете фильтроваться или сортироваться по выбранным полям.

В разделе **Фильтры детальных полей** вы также можете нажать на кнопку **Преобразовать фильтры**, чтобы начать использовать расширенный формат фильтрации. Этот формат позволяет комбинировать условия фильтрации, указанные в различных полях, с помощью логического ИЛИ. После нажатия на кнопку **Преобразовать фильтры**, справа открывается панель. Нажмите на кнопку **Преобразовать фильтры**, подтверждающую отзыв лицензии. Теперь вы можете определить преобразованный фильтр с условиями из раздела **Детальные данные**, которые применяются с помощью логического ИЛИ.

Преобразование отчета в формат, поддерживающий сложные условия фильтрации, сделает его несовместимым с предыдущими версиями Kaspersky Security Center (11 и ниже). Также в преобразованном отчете не будет данных с подчиненных Серверов администрирования с несовместимыми версиями.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.
6. Закройте окно **Редактирование отчета <Название отчета>**.

Измененный шаблон отчета появится в списке шаблонов отчетов.

Экспорт отчета в файл

Вы можете экспортировать отчет в файл формата XML, HTML или PDF.

Чтобы экспортировать отчет в файл:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Установите флажок рядом с названием отчета, который требуется экспортировать в файл.
3. Нажмите на кнопку **Экспортировать отчет**.
4. В открывшемся окне измените имя файла отчета в поле **Имя**. По умолчанию имя файла совпадает с именем выбранного шаблона отчета.
5. Выберите тип файла отчета: XML, HTML или PDF.

   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, программа выводит сообщение о том, что его необходимо установить на Сервер администрирования. Установите инструмент вручную, а затем переходите к следующему шагу.
6. Нажмите на кнопку **Экспортировать отчет**.

   Отчет будет загружен, в выбранном формате, в папку по умолчанию, на ваше устройство, или откроется стандартное окно **Сохранить как** в вашем браузере, чтобы вы могли сохранить файл в нужном вам месте.

Отчет будет сохранен в файл.

Генерация и просмотр отчета

Чтобы сформировать и просмотреть отчет:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Отчеты**.
2. Нажмите на имя шаблона отчета, который вы хотите использовать для создания отчета.

Отображается сгенерированный отчет с использованием выбранного шаблона.

Данные отчета отображаются в соответствии с языком локализации Сервера администрирования.

В сформированных отчетах некоторые шрифты могут некорректно отображаться на диаграммах. Чтобы избежать этого, установите библиотеку fontconfig. Также убедитесь, что в операционной системе установлены шрифты, соответствующие языковому стандарту вашей операционной системы.

В отчете отображаются следующие данные:

- На закладке **Сводная информация**:
  - тип и название отчета, его краткое описание и отчетный период, а также информация о том, для какой группы устройств создан отчет;
  - графическая диаграмма с наиболее характерными данными отчета;
  - сводная таблица с вычисляемыми показателями отчета.

- На закладке **Подробнее** отобразится таблица с подробными данными отчета.

Создание задачи рассылки отчета

Можно создать задачу рассылки выбранных отчетов.

Чтобы создать задачу рассылки отчета:

1. Перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. [Не обязательно] Установите флажки рядом с шаблонами отчетов, на основе которых вы хотите сформировать задачу рассылки отчетов.
3. Нажмите на кнопку **Новая задача рассылки отчетов**.
4. Запустится мастер создания задачи. Для продолжения работы мастера нажмите на кнопку **Далее**.
5. На первой странице мастера укажите название задачи. По умолчанию используется название **Рассылка отчетов (<N>)**, где <N> – это порядковый номер задачи.
6. На странице параметров задачи в мастере укажите следующие параметры:
   a. Шаблоны отчетов, рассылаемых задачей. Если вы их выбрали на шаге 2, пропустите этот шаг.
   b. Формат отчета: HTML, XLS или PDF.

      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, программа 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.
   d. Будут ли отчеты сохраняться в папку вместе с соответствующими параметрами.

      После того как **вы включите параметр Сохранить отчеты в папке**, вам нужно указать POSIX-путь к папке. Если вы хотите сохранить отчеты в папку общего доступа, вам также нужно установить флажок **Задать учетную запись для доступа к папке общего доступа** и указать учетную запись пользователя и пароль для доступа к этой папке.

      > Если вы выбрали сохранение отчетов в папку общего доступа, требуется обеспечить доступ к этой папке с устройства, на котором установлен Сервер администрирования. Способы обеспечения доступа к папке и используемые инструменты зависят от вашей инфраструктуры.

      При сохранении отчетов в локальную папку обычно не требуются учетные данные, поскольку учетная запись, под которой работает Сервер администрирования, имеет доступ к этой папке. При необходимости вы можете указать учетные данные пользователя на шаге мастера **Выбор учетной записи для запуска задачи**.

      Если вы хотите, чтобы новый файл отчета перезаписывал файл, который был сохранен в папке отчетов при предыдущем запуске задачи, вы можете установить флажок **Замещать предыдущие отчеты того же типа**, независимо от выбранной папки.
7. Если требуется изменить другие параметры задачи после ее создания, на странице **Завершение создания задачи** в мастере включите параметр **Открыть окно свойств задачи после ее создания**.
8. Нажмите на кнопку **Создать**, чтобы создать задачу и закрыть мастер.

   Будет создана задача отправки отчета. Если включен параметр **Открыть окно свойств задачи после ее создания**, откроется окно параметров задачи.

Удаление шаблонов отчетов

Чтобы удалить шаблоны отчетов:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Отчеты**.
2. Установите флажки напротив шаблонов отчетов, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **ОК**, чтобы подтвердить свой выбор.

Выбранные шаблоны отчетов будут удалены. Если эти шаблоны отчетов были включены в задачи рассылки отчетов, они также будут удалены из этих задач.

События и выборки событий

В этом разделе содержится информация о событиях и выборках событий, о типах событий, возникших в компонентах Kaspersky Security Center Linux, и об управлении блокировкой частых событий.

О событиях в Kaspersky Security Center Linux

Kaspersky Security Center Linux позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

События по типу

В Kaspersky Security Center Linux существуют следующие типы уведомлений:

- Общие события. Эти события возникают во всех управляемых программах "Лаборатории Касперского". Например, общее событие Вирусная атака. Общие события имеют строго определенные синтаксис и семантику. Общие события используются, например, в отчетах и панели мониторинга.
- Специфические события управляемых программ "Лаборатории Касперского". Каждая управляемая программа "Лаборатории Касперского" имеет собственный набор событий.

События по источнику

Просмотреть полный список событий, которые может генерировать программа, можно на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть список событий в свойствах Сервера администрирования.

События могут генерироваться следующими программами:

- Компоненты программы Kaspersky Security Center Linux:
  - Сервер администрирования
  - Агент администрирования
- Управляемые программы "Лаборатории Касперского"

  Подробнее о событиях, генерируемых управляемыми программами "Лаборатории Касперского", см. в документации соответствующей программы.

События по уровню важности

Каждое событие имеет собственный уровень важности. В зависимости от условий возникновения, событию могут быть присвоены различные уровни важности. Существует четыре уровня важности событий:

- *Критическое событие* – событие, указывающее на возникновение критической проблемы, которая может привести к потере данных, сбою в работе или критической ошибке.
- *Отказ функционирования* – событие, указывающее на возникновение серьезной проблемы, ошибки или сбоя, произошедшего во время работы программы или выполнения процедуры.
- *Предупреждение* – событие, не обязательно являющееся серьезным, однако указывающее на возможное возникновение проблемы в будущем. Чаще всего события относятся к Предупреждениям, если после их возникновения работа программы может быть восстановлена без потери данных или функциональных возможностей.
- *Информационное сообщение* – событие, возникающее с целью информирования об успешном выполнении операции, корректной работе программы или завершении процедуры.

Для каждого события задано время хранения, которое можно посмотреть или изменить в Kaspersky Security Center Linux. 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.

События компонент Kaspersky Security Center Linux

Каждый компонент Kaspersky Security Center Linux имеет собственный набор типов событий. В этом разделе перечислены типы событий, которые происходят на Сервере администрирования Kaspersky Security Center и Агенте администрирования. Типы событий, которые возникают в программах "Лаборатории Касперского", в этом разделе не перечислены.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

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 Linux, 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 Linux 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.

События Сервера администрирования

В этом разделе содержится информация о событиях Сервера администрирования.

Критические события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center с уровнем важности **Критическое**.

Для каждого события, которое может генерировать программа, можно указать параметры уведомлений и параметры хранения на закладке **Настройка событий** в свойствах политики программы. Для Сервера администрирования можно дополнительно просмотреть и настроить список событий в свойствах Сервера администрирования. Если вы хотите настроить параметры уведомлений сразу для всех событий, настройте общие параметры уведомлений в свойствах Сервера администрирования.

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 Linux проверяет, не превышено ли лицензионное ограничение. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии превышает 110% от общего количества лицензионных единиц, 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 Linux определяет правила генерации событий при превышении лицензионного ограничения.	180 дней
Устройство стало	4111	KLSRV_HOST_OUT_CONTROL	События этого типа возникают, если управляемое устройство видимо в сети,	180 дней

неуправляемым			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.	
Статус устройства "Критический"	4113	KLSRV_HOST_STATUS_CRITICAL	События этого типа возникают, если управляемому устройству назначен статус *Критический*. Вы можете настроить условия 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 скоро истекает	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	События этого типа возникают, если приближается дата окончания срока действия коммерческой лицензии. Один раз в день Kaspersky Security Center проверяет, не истек ли срок действия лицензии. События этого типа публикуются за 30 дней, 15 дней, 5 дней и 1 день, до истечения срока действия лицензии. Это количество дней нельзя изменить. Если Сервер администрирования выключен, в указанный день окончания срока действия лицензии, событие не будет опубликовано до следующего дня. После окончания срока действия коммерческой лицензии, Kaspersky Security Center Linux работает в режиме Базовой функциональности. Вы можете ответить на событие следующими способами: • Убедитесь, что резервный лицензионный ключ добавлен на Сервер администрирования. • Если вы используете подписку, 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

События отказа функционирования Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Linux с уровнем важности **Отказ функционирования**.

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
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. • Проверить, были ли изменены имя пользователя и/или пароль к папкам. • Проверьте подключение к интернету, так как это может быть причиной события. Следуйте инструкциям по обновлению баз и программных модулей.	180 дней
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. 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	180 дней

			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.	

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:
			• Вы используете SQL Server Express Edition:
			  • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой версии. Возможно, ваша база данных Сервера администрирования превысила ограничение размера базы данных.
			  • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования.
			  • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Linux, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования.
			• Вы используете СУБД, отличную от SQL Server Express Edition:
			  • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования.
			  • Сократите список событий для хранения в базе данных Сервера администрирования.
			Просмотрите информацию о выборе СУБД.
				180 дней

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Linux с уровнем важности **Предупреждение**.

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.	90 дней
Лицензионное ограничение превышено	4098	KLSRV_EV_LICENSE_CHECK_100_110	Один раз в день Kaspersky Security Center Linux проверяет, не превышено ли лицензионное ограничение. События этого типа возникают, если Сервер администрирования регистрирует превышение лицензионного ограничения программ "Лаборатории Касперского", установленных на клиентских устройствах, и если количество используемых лицензионных единиц одной лицензии 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 Linux определяет правила генерации событий при превышении лицензионного ограничения.	90 дней
Устройство долго не проявляет активности в сети	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	События этого типа возникают, если управляемое устройство неактивно в течение некоторого времени. Чаще всего это происходит, когда управляемое устройство выводится из эксплуатации. Вы можете ответить на событие следующими способами: • Удалите устройство из списка управляемых устройств вручную. Укажите интервал, по истечении которого создается событие **Устройство долго не проявляет активности в сети** с помощью Kaspersky Security Center 14 Web Console.	90 дней

			• Укажите интервал, по истечении которого устройство автоматически удаляется из группы с помощью Kaspersky Security Center 14 Web Console.	
Конфликт имен устройств	4102	KLSRV_EVENT_HOSTS_CONFLICT	События этого типа возникают, если Сервер администрирования рассматривает два или более управляемых устройства как одно устройство. Чаще всего это происходит, когда клонированный жесткий диск использовался для развертывания программ на управляемых устройствах и без переключения Агента администрирования в режим клонирования выделенного диска на эталонном устройстве. Чтобы избежать этой проблемы, перед клонированием жесткого диска этого устройства переключите Агент администрирования в режим клонирования диска на эталонном устройстве.	90 дней
Статус устройства "Предупреждение"	4114	KLSRV_HOST_STATUS_WARNING	События этого типа возникают, если управляемому устройству назначен статус *Предупреждение*. Вы можете настроить условия при выполнении которых, статус устройства изменяется на *Предупреждение*.	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	90 дней

			для интеграции с PKI и для выпуска сертификата. Просмотрите свойства учетной записи.	
Сертификат удален	4134	KLSRV_CERTIFICATE_REMOVED	События этого типа возникают, если администратор удаляет сертификат любого типа (общий, почтовый, VPN) для Управления мобильными устройствами. 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 (см. главу "Downstream message error response codes").	90 дней
HTTP-ошибка при отправке FCM-сообщения на FCM-сервер	4139	KLSRV_GCM_HTTP_ERROR	События этого типа возникают, если Управление мобильными устройствами настроено на использование Google Firebase Cloud Messaging (FCM) для подключения управляемых	90 дней

			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 (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.	
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
Мало свободного места в базе Сервера администрирования	4106	KLSRV_NO_SPACE_IN_DATABASE	События этого типа возникают, если свободное место в базе Сервера администрирования ограничено. Если вы не устраните эту проблему, скоро база данных Сервера администрирования достигнет своей емкости и Сервер администрирования не будет работать. Ниже приведены причины возникновения события, которые зависят от используемой СУБД, и соответствующие способы реагирования на событие. Вы используете SQL Server Express Edition: • Проверьте в документации к SQL Server Express ограничение размера базы данных для используемой	90 дней

			версии. Возможно, ваша база данных Сервера администрирования достигла ограничения размера базы данных. • Ограничьте количество событий, хранящихся в базе данных Сервера администрирования. • В базе данных Сервера администрирования слишком много событий, отправленных компонентом Контроль программ. Вы можете изменить параметры политики Kaspersky Endpoint Security для Linux, касающиеся хранения событий компонента Контроль программ в базе данных Сервера администрирования. Вы используете СУБД, отличную от SQL Server Express Edition: • Не ограничивайте количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования. Просмотрите информацию о выборе СУБД.	
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 программ "Лаборатории Касперского"	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	События этого типа возникают, если Сервер администрирования регистрирует новые обновления программ "Лаборатории Касперского", установленных на управляемых устройствах, для установки которых требуется одобрение. Одобрите или отклоните обновления с помощью Kaspersky Security Center Web Console.	90 дней
Превышено ограничение числа	4145	KLSRV_EVP_DB_TRUNCATING	События такого типа возникают, если удаление старых событий из	Не хранится

событий, началось удаление событий из базы данных			базы данных Сервера администрирования началось после достижения максимального количества событий, хранящихся в базе данных Сервера администрирования. Вы можете ответить на событие следующими способами: • Укажите максимальное количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	
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. Вы можете ответить на событие следующими способами: • Укажите максимально допустимое количество событий, хранящихся в базе данных Сервера администрирования. • Сократите список событий для хранения в базе данных Сервера администрирования.	Не хранится

Информационные события Сервера администрирования

В таблице ниже приведены события Сервера администрирования Kaspersky Security Center Linux с уровнем важности **Информационное сообщение**.

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	
Обнаружено 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	
Появились файлы для отправки на анализ в "Лабораторию Касперского"	4131	KLSRV_APS_FILE_APPEARED	30 дней	
Идентификатор экземпляра FCM	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 дней	

мобильного устройства изменен				
Обновления успешно скопированы в заданную папку	4122	KLSRV_UPD_REPL_OK	30 дней	
Установлено соединение с подчиненным Сервером администрирования	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 дней	
Установлено соединение с главным Сервером администрирования	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 дней	
Базы обновлены	4144	KLSRV_UPD_BASES_UPDATED	30 дней	
Аудит: Подключение к Серверу администрирования	4147	KLAUD_EV_SERVERCONNECT	30 дней	События этого типа возникают при подключении пользователя к Серверу администрирования с помощью Консоли администрирования или Web Console. Такие события включают IP-адрес устройства, на котором установлена Консоль администрирования на основе консоли Microsoft Management Console (MMC) или Сервер Web Console.
Аудит: Изменение объекта	4148	KLAUD_EV_OBJECTMODIFY	30 дней	Это событие отслеживает изменения в следующих объектах: • Группа администрирования • Группа безопасности • Пользователь • Инсталляционный пакеты • Задача • Политика • Сервер • Виртуальный Сервер
Аудит: Изменение статуса объекта	4150	KLAUD_EV_TASK_STATE_CHANGED	30 дней	Например, это событие возникает, если задача завершилась ошибкой.
Аудит: Изменение параметров группы	4149	KLAUD_EV_ADMGROUP_CHANGED	30 дней	
Аудит: Подключение к Серверу администрирования было прервано	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

События Агента администрирования

В этом разделе содержится информация о событиях Агента администрирования.

События предупреждения Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center Linux с уровнем важности **Предупреждение**.

События предупреждения Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Произошел инцидент	549	GNRL_EV_APP_INCIDENT_OCCURED	30 дней

Информационные события Агента администрирования

В таблице ниже приведены события Агента администрирования Kaspersky Security Center Linux с уровнем важности **Информационное сообщение**.

Информационные события Агента администрирования

Отображаемое имя типа события	Идентификатор типа события	Тип события	Срок хранения по умолчанию
Установлена программа	7703	KLNAG_EV_INV_APP_INSTALLED	30 дней
Программа удалена	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 дней
Установлена наблюдаемая программа	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 дней
Удалена наблюдаемая программа	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 дней
Новое устройство добавлено	7708	KLNAG_EV_DEVICE_ARRIVAL	30 дней
Устройство удалено	7709	KLNAG_EV_DEVICE_REMOVE	30 дней
Обнаружено новое устройство	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 дней
Устройство авторизовано	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 дней

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**, **Отказы функционирования**, **Предупреждения** и **Информационные события**.
- Время: **Последние события**.
- Тип: **Запросы пользователей** и **События аудита**.

Вы можете создавать и просматривать определенные пользователем выборки событий на основе параметров, доступных для настройки в интерфейсе Kaspersky Security Center 14 Web Console.

Выборки событий доступны в Kaspersky Security Center 14 Web Console в разделе **Мониторинг и отчеты** → **Выборки событий**.

По умолчанию выборки событий включают информацию за последние семь дней.

Kaspersky Security Center Linux имеет набор выборок (предопределенных) по умолчанию:

- События с разным уровнем важности:
  - **Критические события.**
  - **Отказ функционирования.**
  - **Предупреждения.**
  - **Информационные сообщения.**
- **Запросы пользователей** (события управляемых программ).

- **Последние события** (за последнюю неделю).
- **События аудита**.

Вы можете также создавать и настраивать дополнительные пользовательские выборки событий. В пользовательских выборках вы можете фильтровать события по свойствам устройств, в которых они возникли (по именам устройств, IP-диапазонам и группам администрирования), по типам событий и уровням важности, по названию программы и компонента, а также по временному интервалу. Также можно включить результаты задачи в область поиска. Вы также можете использовать поле поиска, в котором можно ввести слово или несколько слов. Отображаются все события, содержащие любые введенные слова в любом месте их свойств (таких как имя события, описание, имя компонента).

Как для предопределенных выборок, так и для пользовательских выборок вы можете ограничить количество отображаемых событий или количество записей для поиска. Оба варианта влияют на время, за которое Kaspersky Security Center Linux отображает события. Чем больше база данных, тем более трудоемким может быть процесс.

Вы можете выполнить следующее:

- Изменить параметры выборки событий.
- Сгенерировать выборки событий.
- Просмотреть сведения о выбранных выборках событий.
- Удалить выборки событий.
- Удалить события из базы данных Сервера администрирования.

Создание выборки событий

Чтобы создать выборку событий:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Нажмите на кнопку **Добавить**.
3. В открывшемся окне **Новая выборка событий** укажите параметры новой 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.

Изменение выборки событий

Чтобы изменить выборку событий:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется изменить.
3. Нажмите на кнопку **Свойства**.

   Откроется окно свойств выборки событий.
4. Отредактируйте свойства выборки событий.

   > Для предопределенной выборки событий можно изменять свойства только на следующих закладках: **Общие** (за исключением имени выборки), **Время** и **Права доступа**.

   Для пользовательских выборок можно редактировать все свойства.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Измененная выборка событий отображается в списке.

Просмотр списка выборки событий

Просмотр выборки событий:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажок напротив выборки событий, которую требуется запустить.
3. Выполните одно из следующих действий:
   - Чтобы настроить сортировку для результатов выборки событий:
     a. Нажмите на кнопку **Изменить сортировку и запустить**.
     b. В отобразившемся 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.

Просмотр информации о событии

Чтобы просмотреть детальную информацию о событии:

1. Запустите выборку событий.
2. Нажмите на требуемое событие.
   Откроется окно **Свойства события**.
3. В открывшемся окне можно выполнить следующие действия:
   - Просмотреть информацию выбранного события.
   - Перейти к следующему или к предыдущему событию в списке – результате выборки событий.
   - Перейти к устройству, на котором возникло событие.
   - Перейти к группе администрирования, содержащей устройство, на котором возникло событие.
   - Для события, связанного с задачей, перейдите в свойства задачи.

Экспорт событий в файл

Чтобы экспортировать события в файл:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **Экспортировать в файл**.

Выбранные события экспортированы в файл.

Просмотр истории объекта из события

Из события создания или события изменения объекта, которое поддерживает управление ревизиями, вы можете перейти к истории ревизий объекта.

Чтобы просмотреть историю объекта из события:

1. Запустите выборку событий.
2. Установите флажок рядом с требуемым событием.
3. Нажмите на кнопку **История ревизий**.

Откроется история ревизий объекта.

Удаление событий

Чтобы удалить одно или несколько событий:

1. Запустите выборку событий.
2. Установите флажки рядом с требуемыми событиями.
3. Нажмите на кнопку **Удалить**.

Выбранные события удалены и не могут быть восстановлены.

Удаление выборок событий

Можно удалять только пользовательские выборки событий. Предопределенные выборки событий нельзя удалить.

Чтобы удалить выборки событий:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты → Выборки событий**.
2. Установите флажки напротив выборок событий, которые требуется удалить.
3. Нажмите на кнопку **Удалить**.
4. В появившемся окне нажмите на кнопку **OK**.

Выборка событий будет удалена.

Настройка срока хранения события

Kaspersky Security Center Linux позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования. Возможно, вам нужно хранить некоторые события в течение более длительного или более короткого периода, чем указано по умолчанию. Вы можете изменить срок хранения события по умолчанию.

Если вас не интересует сохранение каких-либо событий в базе данных Сервера администрирования, вы можете выключить соответствующий параметр в политике Сервера администрирования, политике программы "Лаборатории Касперского" или в свойствах Сервера администрирования (только для событий Сервера администрирования). Это уменьшит количество типов событий в базе данных.

Чем больше срок хранения события, тем быстрее база данных достигает максимального размера. Однако более длительный срок хранения события позволяет выполнять задачи мониторинга и просматривать отчеты в течение более длительного периода.

Чтобы задать срок хранения события в базе данных Сервера администрирования:

1. Выберите **Устройства → Политики и профили политик**.
2. Выполните одно из следующих действий:
   - Чтобы настроить срок хранения событий Агента администрирования или управляемой программы "Лаборатории Касперского" нажмите на имя соответствующей политики.

     Откроется страница свойств политики.
   - Чтобы настроить события Сервера администрирования, в верхней части экрана нажмите на значок параметров ( ) рядом с именем требуемого Сервера администрирования.

     Если у вас есть политика для Сервера администрирования, вы можете нажать на название этой политики.

     Откроется страница свойств Сервера администрирования (или страница свойств политики Сервера администрирования).
3. Выберите закладку **Настройка событий**.

   Отображается раздел **Критическое** со списком связанных событий.
4. Выберите раздел **Отказ функционирования**, **Предупреждение** или **Информационное сообщение**.
5. В списке типов событий на правой панели перейдите по ссылке с названием события, срок хранения которого вы хотите изменить.

   В открывшемся окне в разделе **Регистрация событий** включите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.
6. В поле редактирования под переключателем укажите количество дней для сохранения события.

7. Если вы не хотите сохранять событие в базе данных Сервера администрирования, выключите параметр **Хранить в базе данных Сервера администрирования в течение (сут)**.

   Если вы настраиваете события Сервера администрирования в окне свойств Сервера администрирования и если параметры событий заблокированы в политике Сервера администрирования Kaspersky Security Center Linux, вы не сможете изменить значение срока хранения события.

8. Нажмите на кнопку **OK**.

   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.

О блокировке частых событий

Управляемая программа, например Kaspersky Endpoint Security для Linux, установленная на одном или нескольких управляемых устройствах, может отправлять на Сервер администрирования множество однотипных событий. Прием частых событий может привести к перегрузке базы данных Сервера администрирования и перезаписи других событий. Сервер администрирования начинает блокировать наиболее частые события, когда количество всех полученных событий превышает установленное ограничение для базы данных.

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 получение событий такого типа.
- Если вы хотите, например, выяснить причину отправки частых событий на Сервер администрирования, вы можете разблокировать 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 частых событий.

Управление блокировкой частых событий

Сервер администрирования автоматически блокирует получение частых событий, но вы можете разблокировать и продолжать получать частые события. Также можно заблокировать получение частых событий, которые вы разблокировали ранее.

Чтобы управлять блокировкой частых событий:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий**:

   - Если вы хотите разблокировать прием частых событий:

     a. Выберите частые события, который нужно разблокировать, и нажмите на кнопку **Исключить**.

     b. Нажмите на кнопку **Сохранить**.

   - Если вы хотите заблокировать прием частых событий:

     a. Выберите частые события, которые вы хотите заблокировать и нажмите на кнопку **Заблокировать**.

     b. Нажмите на кнопку **Сохранить**.

Сервер администрирования принимает разблокированные частые события и не принимает заблокированные частые события.

Отмена блокировки частых событий

Вы можете отменить блокировку частых событий и начать получение событий до тех пор, пока Сервер администрирования снова не заблокирует эти частые события.

Чтобы отменить блокировку частых событий:

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

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** выберите раздел **Блокировка частых событий**.

3. В разделе **Блокировка частых событий** нажмите строку частого события, для которого вы хотите отменить блокировку.

4. Нажмите на кнопку **Отменить блокировку**.

Частое событие удаляется из списка частых событий. Сервер администрирования будет получать события этого типа.

Обработка и хранение событий на Сервере администрирования

Информация о событиях, возникших в работе программы и управляемых устройств, сохраняется в базе данных Сервера администрирования. Каждое событие относится к определенному типу и уровню важности (*Критическое событие*, *Отказ функционирования*, *Предупреждение*, *Информационное сообщение*). В зависимости от условий, при которых произошло событие, программа может присваивать событиям одного типа разные уровни важности.

Вы можете просматривать типы и уровни важности событий в разделе **Настройка событий** окна свойств Сервера администрирования. В разделе **Настройка событий** вы также можете настроить параметры обработки каждого события Сервером администрирования:

- регистрацию событий на Сервере администрирования и в журналах событий операционной системы на устройстве и на Сервере администрирования;
- способ уведомления администратора о событии (например, SMS, сообщение электронной почты).

В разделе **Хранилище событий** окна свойств Сервера администрирования можно настроить параметры хранения событий в базе данных Сервера администрирования: ограничить количество записей о событиях и время хранения записей. Когда вы указываете максимальное количество событий, программа 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.

Программа проверяет базу данных каждые 10 минут. Если количество событий достигает на 10 000 больше указанного максимального значения, программа удаляет самые старые события, чтобы осталось только указанное максимальное количество событий.

Когда Сервер администрирования удаляет старые события, он не может сохранять новые события в базе данных. В течение этого периода информация о событиях, которые были отклонены, записывается в журнал событий операционной системы. Новые события помещаются в очередь, а затем сохраняются в базе данных после завершения операции удаления. По умолчанию очередь событий ограничена 20 000 событиями. Вы можете настроить ограничение очереди, изменив значение флага KLEVP_MAX_POSTPONED_CNT.

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.

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 и отвечая на них в режиме реального времени.

Уведомления по электронной почте, SMS и запуском исполняемого файла или скрипта

Kaspersky Security Center Linux 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.

Получив уведомление по SMS или по электронной почте, вы можете принять решение о своем ответе на событие. Этот ответ должен быть наиболее подходящим для сети вашей организации. Запустив исполняемый файл или скрипт, вы заранее определяете ответ на событие. Вы также можете рассмотреть запуск исполняемого файла или скрипта в качестве основного ответа на событие. После запуска исполняемого файла вы можете предпринять другие шаги для ответа на событие.

Просмотр экранных уведомлений

Вы можете просматривать экранные уведомления тремя способами:

- В разделе **Мониторинг и отчеты** → **Уведомления**. Здесь вы можете просмотреть уведомления, относящиеся к предопределенным категориям.
- В отдельном окне, которое можно открыть независимо от того, какой раздел вы используете в данный момент. В этом случае вы можете отметить уведомления как просмотренные.
- В веб-виджете **Уведомления, выбранные по уровню важности** в разделе **Мониторинг и отчеты** → **Панель мониторинга**. В этом веб-виджете вы можете просматривать только уведомления с уровнями важности *Критическое* и *Предупреждение*.

Вы можете выполнять действия, например, вы можете ответить на событие.

Чтобы просмотреть уведомления предопределенной категории:

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Уведомления**.

   На левой панели выбрана категория **Все уведомления**, а справа отображаются все уведомления.

2. На левой панели выберите одну из следующих категорий:

   - **Развертывание**
   - **Устройства**
   - **Защита**
   - **Обновления** (сюда входят уведомления о доступных для загрузки программах "Лаборатории Касперского" и уведомления о загруженных обновлениях антивирусных баз)
   - **Защита от эксплойтов**
   - **Сервер администрирования** (это уведомление включает в себя события, относящиеся только к Серверу администрирования)
   - **Полезные ссылки** (сюда входят ссылки на ресурсы "Лаборатории Касперского", например, ссылка на Службу технической поддержки "Лаборатории Касперского", на форум "Лаборатории Касперского", на страницу продления лицензии или на Вирусную энциклопедию)
   - **Корпоративные новости "Лаборатории Касперского"** (сюда входит информация о выпусках программ "Лаборатории Касперского")

   В списке уведомлений отобразится выбранная категория. Список содержит следующее:

- Значок, относящийся к теме уведомления: развертывание, защита, обновления, управление устройствами, Защита от эксплойтов, Сервер администрирования.
- Уровень важности уведомления. Отображаются уведомления со следующими уровнями важности: **Критические уведомления**, **Предупреждающие уведомления**, **Информационные уведомления**. Уведомления в списке сгруппированы по уровню важности.
- **Уведомление**. Здесь содержится описание уведомления.
- **Действие**. Здесь содержится ссылка на быстрое действие, которое рекомендуется выполнить. Например, по этой ссылке вы можете перейти к хранилищу и установить программу безопасности на устройства, просмотреть список устройств или список событий. После того, как вы

выполнили рекомендуемое действие для уведомления, этому уведомлению присваивается статус *Просмотрено*.

- **Зарегистрированный статус**. Здесь содержится количество дней или часов, прошедших с даты регистрации уведомления на Сервере администрирования.

Чтобы просмотреть экранные уведомления в отдельном окне по уровню важности:

1. Нажмите на значок флага () в правом верхнем углу Kaspersky Security Center 14 Web Console.

   Если около значка флажка есть красная точка, значит, есть непросмотренные уведомления.

   Откроется окно со списком уведомлений. По умолчанию выбрана закладка **Все уведомления** и отображаются уведомления, сгруппированные по уровням важности: *Критические уведомления*, *Предупреждающие уведомления* и *Информационные уведомления*.

2. Выберите закладку **Система**.

   Отображается список уведомлений с уровнями важности *Критические уведомления* () и *Предупреждающие уведомления* (). Список уведомление включает следующее:

   - Цветной индикатор. Критические уведомления отмечены красным. Предупреждающие уведомления отмечены желтым.
   - Значок, относящийся к теме уведомления: развертывание (), защита (), обновления(), управление устройствами (), Защита от эксплойтов (), Сервер администрирования ().
   - Описание уведомления.
   - Значок флажка. Серый флаг используется для уведомлений, которым присвоен статус *Не просмотрено*. Когда вы выбираете серый флаг и назначаете статус *Просмотрено* для уведомления, цвет флажка изменится на белый.
   - Ссылка на рекомендуемое действие. Когда вы выполняете рекомендуемое действие, переходя по ссылке, уведомлению присваивается статус *Просмотрено*.
   - Количество дней, прошедших с даты регистрации уведомления на Сервере администрирования.

3. Выберите закладку **Больше**.

   Отображается список уведомлений с уровнем важности *Информационное уведомление*.

   Структура списка такая же, как и для списка на закладке **Система** (описание приведено выше). Отличается только отсутствием цветного индикатора.

Вы можете фильтровать уведомления по датам, когда они были зарегистрированы на Сервере администрирования. Используйте флажок **Показать фильтр**, чтобы настроить фильтр.

Чтобы просмотреть экранные уведомления на веб-виджете:

1. В разделе **Панель мониторинга** выберите **Добавить или восстановить веб-виджет**.

2. В открывшемся окне нажмите на категорию **Другие**, выберите веб-виджет **Уведомления, выбранные по уровню важности** и нажмите на кнопку Добавить.

   Веб-виджет отображается на закладке **Панель мониторинга**. По умолчанию на веб-виджете отображаются уведомления с уровнем важности *Критическое*.

   Вы можете нажать на кнопку **Параметры** на веб-виджете и изменить параметры веб-виджета, 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** в разделе **Мониторинг и отчеты**.

О статусах устройства

Kaspersky Security Center Linux 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 Linux учитывает видимость устройства в сети (см. таблицу ниже). Если Kaspersky Security Center Linux 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.

Условия присвоения статусов устройству

Условие	Описание условия	Доступные значения
Программа безопасности не установлена	Агент администрирования установлен на устройстве, но не установлена программа безопасности.	• Переключатель включен. • Переключатель выключен.
Обнаружено 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.
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 вирусов	Устройство видимо в сети и на устройстве установлена программа безопасности, но ни задача *Поиск вредоносного ПО*, ни задача локальной проверки не выполнялись больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования семь дней назад или ранее.	Более 1 дня.
Базы устарели	Устройство видимо в сети и на устройстве установлена программа безопасности, но антивирусные базы не обновлялись на этом устройстве больше указанного времени. Условие применимо только к устройствам, которые были добавлены в базу данных Сервера администрирования день назад или ранее.	Более 1 дня.
Давно не подключались	Агент администрирования установлен на устройстве, но устройство не подключалось к Серверу администрирования больше указанного времени, так как устройство выключено.	Более 1 дня.
Обнаружены активные угрозы	Количество необработанных объектов в папке **Активные угрозы** превышает указанное значение.	Более чем 0 штук.
Требуется перезагрузка	Устройство видимо в сети, но программа требует перезагрузки устройства дольше указанного времени, по одной из выбранных причин.	Более чем 0 минут.
Установлены несовместимые программы	Устройство видимо в сети, но при инвентаризации программного обеспечения, выполненной Агентом администрирования, на устройстве были обнаружены установленные несовместимые программы.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии истек	Устройство видимо в сети, но срок действия лицензии истек.	• Переключатель выключен. • Переключатель включен.
Срок действия лицензии скоро истекает	Устройство видимо в сети, но срок действия лицензии истекает менее чем через указанное количество дней.	Более чем 0 дней.
Есть необработанные инциденты	На устройстве есть необработанные инциденты. Инциденты могут быть созданы как автоматически, с помощью установленных на клиентском устройстве управляемых программ "Лаборатории Касперского", так и вручную администратором.	• Переключатель выключен.

		• Переключатель включен.
Статус устройства определен программой	Статус устройства определяется управляемой программой.	• Переключатель выключен. • Переключатель включен.
На устройстве заканчивается дисковое пространство	Свободное дисковое пространство устройства меньше указанного значения или устройство не может быть синхронизировано с Сервером администрирования. Статусы *Критический* или *Предупреждение* меняются на статус *OK*, 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 программа безопасности на устройстве отключена больше указанного времени. В этом случае состояние программы безопасности *Остановлена* или *Сбой* и отличается от следующих: *Запускается*, *Выполняется* или *Приостановлена*.	Более чем 0 минут.
Программа безопасности не запущена	Устройство видимо в сети и программа безопасности установлена на устройстве, но не запущена.	• Переключатель выключен. • Переключатель включен.

Kaspersky Security Center Linux 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 *OK*.

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 Linux с предыдущей версии, значение условия **Базы устарели** для назначения статуса *Критический* или *Предупреждение* не изменится.

Когда Kaspersky Security Center Linux присваивает устройству статус, для некоторых условий (см. графу "Описание условий") учитывается видимость устройств в сети. Например, если управляемому устройству был присвоен статус *Критический*, так как выполнено условие Базы устарели, а затем для устройства стало видимо в сети, то устройству присваивается статус *OK*.

Настройка переключения статусов устройств

Вы можете изменить условия присвоения статусов *Критический* или *Предупреждение* устройству.

Чтобы изменить статус устройства на Критический:

1. В главном окне программы перейдите в раздел **Устройства → Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите закладку **Статус устройства**.
4. Выберите раздел **Критический**.
5. В блоке **Установить статус "Критический", если** включите условие, чтобы переключить устройство в состояние *Критическое*.

   Вы можете изменить параметры, которые не заблокированы в родительской политике.

6. Установите переключатель рядом с условием в списке.

7. Нажмите на кнопку **Изменить** в верхнем левом углу списка.
8. Для выбранного условия установите необходимое вам значение.
   Не для всех условий можно задать значения.
9. Нажмите на кнопку **ОК**.

При невыполнении заданных условий управляемому устройству присваивается статус *Критический*.

Чтобы изменить статус устройства на Предупреждение:

1. В главном окне программы перейдите в раздел **Устройства** → **Иерархия групп**.
2. В открывшемся списке групп перейдите по ссылке с названием группы, для которой вы хотите изменить переключение статусов устройств.
3. В отобразившемся окне свойств выберите закладку **Статус устройства**.
4. Выберите раздел **Предупреждение**.
5. В блоке **Установить статус "Предупреждение", если**, включите условие, чтобы переключить устройство в состояние *Предупреждение*.

   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*.

Настройка параметров доставки уведомлений

Развернуть все | Свернуть все

Вы можете настроить уведомления о событиях, возникающих в Kaspersky Security Center Linux. В зависимости от выбранного способа уведомления доступны следующие типы уведомлений:

- Электронная почта – при возникновении события программа Kaspersky Security Center Linux посылает уведомление на указанные адреса электронной почты.
- SMS – при возникновении события программа Kaspersky Security Center Linux 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 Linux:

1. В главном меню нажмите на значок параметров () рядом с именем требуемого Сервера администрирования.
   Откроется окно свойств Сервера администрирования на закладке **Общие**.
2. Перейдите в раздел **Уведомление** и на правой панели выберите закладку с требуемым способом уведомления:
   - Электронная почта

     На закладке **Электронная почта** можно настроить уведомления о событиях по электронной почте.

     В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:
     - IPv4-адрес или IPv6-адрес;
     - DNS-имя SMTP-сервера.

     В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

     Если вы включите параметр **Использовать DNS и MX поиск**, вы сможете использовать несколько MX-записей IP-адреса для одного и того же DNS-имени SMTP-сервера. Одно DNS-имя может иметь несколько MX-записей с различными приоритетами полученных электронных писем. Сервер администрирования пытается отправлять уведомления по электронной почте на SMTP-сервер в порядке возрастания приоритета MX-записей.

Если вы включили параметр **Использовать DNS и MX поиск** и не разрешили использование параметров TLS, рекомендуется использовать параметры DNSSEC на вашем серверном устройстве в качестве дополнительной меры защиты при отправке уведомлений по электронной почте.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали 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 Linux проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center Linux 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 тестовое сообщение** можно проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения на указанные адреса электронной почты.

В поле **Получатели (адреса электронной почты)** укажите адреса электронной почты, на которые будут отправляться уведомления. В этом поле можно указать несколько адресов через точку с запятой.

В поле **Тема** укажите тему электронной почты. Вы можете оставить поле пустым.

В раскрывающемся списке **Тема шаблона** выберите шаблон для темы 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 окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Текст уведомления** содержится стандартный текст уведомления о событии, отправляемый программой при возникновении события. Текст содержит подстановочные параметры, такие как имя события, имя устройства и имя домена. Текст сообщения можно изменить, добавив подстановочные параметры с подробными данными события.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

- SMS

На закладке **SMS** можно настроить отправку SMS-уведомлений о различных событиях на мобильный телефон. SMS-сообщения отправляются через почтовый шлюз.

В поле **SMTP-серверы** укажите адреса почтовых серверов через точку с запятой. Вы можете использовать следующие значения параметра:

- IPv4-адрес или IPv6-адрес;
- DNS-имя SMTP-сервера.

В поле **Порт SMTP-сервера** укажите номер порта подключения к SMTP-серверу. По умолчанию установлен порт 25.

Если параметр **Использовать ESMTP-аутентификацию** включен, вы можете указать параметры ESMTP-аутентификации в полях **Имя пользователя** и **Пароль**. По умолчанию параметр не выбран и параметры ESMTP-аутентификации недоступны.

Вы можете указать параметры подключения TLS для SMTP-сервера:

- **Не использовать TLS**

Вы можете выбрать этот параметр, если хотите выключить шифрование сообщений электронной почты.

- **Использовать TLS, если поддерживается SMTP-сервером**

Вы можете выбрать этот параметр, если хотите использовать TLS для подключения к SMTP-серверу. Если SMTP-сервер не поддерживает TLS, Сервер администрирования подключает SMTP-сервер без использования TLS.

- **Всегда использовать TLS, для проверки срока действия сертификата сервера**

Вы можете выбрать этот параметр, если хотите использовать параметры TLS-аутентификации. Если SMTP-сервер не поддерживает TLS, Сервер администрирования не сможет подключиться к SMTP-серверу.

Рекомендуется использовать этот параметр для защиты соединения с SMTP-сервером. Если вы выберете этот параметр, вы можете установить параметры аутентификации для TLS-соединения.

Если вы выбрали 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 файл сертификата SMTP-сервера, 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 Linux проверяет, подписан ли сертификат SMTP-сервера также доверенным центром сертификации. Kaspersky Security Center Linux 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 окне **Адрес электронной почты отправителя: если параметр не задан, будет использоваться адрес получателя. Внимание: не рекомендуется указывать в этом поле несуществующий адрес электронной почты** укажите адрес отправителя электронной почты. Если вы оставите поле пустым, по умолчанию используется адрес получателя. Не рекомендуется использовать несуществующий адрес.

В поле **Номера телефонов получателей SMS-сообщений** укажите номера мобильных телефонов для получения SMS.

В поле **Текст уведомления** напишите текст уведомления о событии, отправляемый программой при возникновении события. Текст может содержать подстановочные параметры, такие как имя события, имя устройства и имя домена.

Если текст уведомления содержит знак процента (%), его нужно указать его два раза подряд, чтобы сообщение было отправлено. Например, "Загрузка процессора составляет 100%%".

Нажмите на кнопку **Отправить тестовое сообщение**, чтобы проверить правильно ли настроены сообщения: программа отправляет тестовые сообщения указанным получателям.

Перейдите по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

- Исполняемый файл для запуска

Если выбран этот способ уведомления, в поле ввода можно указать, какая программа будет запущена при возникновении события.

В поле **Исполняемый файл, который запустится на Сервере администрирования при возникновении события** укажите папку и имя файла, который запустится. Перед указанием файла подготовьте файл и укажите подстановочные параметры, которые определяют сведения о событии, которые будут отправлены в сообщении. Указанные папка и файл должны находиться на Сервере администрирования.

При переходе по ссылке **Настроить ограничение количества уведомлений** можно указать максимальное количество уведомлений, которое программа может отправлять за указанный интервал времени.

3. На закладке настройте параметры уведомлений.
4. Нажмите на кнопку **OK**, чтобы закрыть окно свойств Сервера администрирования.

Сохраненные параметры доставки уведомлений применяются ко всем событиям, которые возникают в Kaspersky Security Center Linux.

Можно изменить значения параметров доставки уведомлений для определенных событий в разделе **Настройка событий** в параметрах Сервера администрирования, параметрах политики или параметрах программы.

Проверка распространения уведомлений

Для проверки распространения уведомлений о событиях используется уведомление об обнаружении тестового "вируса" Eicar на клиентских устройствах.

Чтобы проверить распространение уведомлений о событиях:

1. Остановите задачу постоянной защиты файловой системы на клиентском устройстве и скопируйте тестовый "вирус" Eicar на клиентское устройство. Затем снова включите задачу постоянной защиты файловой системы.
2. Запустите задачу проверки клиентских устройств для группы администрирования или набора устройств, в который входит клиентское устройство с тестовым "вирусом" Eicar.

   Если задача проверки настроена верно, в процессе ее выполнения тестовый "вирус" будет обнаружен. Если параметры уведомлений настроены верно, вы получите уведомление о найденном вирусе.

Чтобы открыть запись об обнаружении тестового "вируса":

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Выборки событий**.
2. Нажмите на название выборки **Последние события**.

   В открывшемся окне отображается уведомление о тестовом "вирусе".

Тестовый "вирус" Eicar не содержит программного кода, который может навредить вашему устройству. При этом большинство программ безопасности компаний-производителей идентифицируют его как вирус. Загрузить тестовый "вирус" можно с официального веб-сайта организации EICAR.

Уведомление о событиях с помощью исполняемого файла

Kaspersky Security Center Linux 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 (см. таблицу ниже).

Подстановочные параметры для описания события

Подстановочный параметр	Описание подстановочного параметра
%SEVERITY%	Уровень важности события. Возможные значения: • **Информационное сообщение** • **Предупреждение** • **Сбой** • **Критическое**
%COMPUTER%	Имя устройства, на котором произошло событие. Максимальная длина имени устройства равна 256 символов.
%DOMAIN%	Имя домена устройства, на котором произошло событие.
%EVENT%	Имя типа события. Максимальная длина названия типа события равна 50 символов.

%DESCR%	Описание события. Максимальная длина описания равна 1000 символов.
%RISE_TIME%	Время создания события.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Название задачи. Максимальная длина названия задачи равна 100 символов.
%KL_PRODUCT%	Название программы.
%KL_VERSION%	Номер версии программы.
%KLCSAK_EVENT_SEVERITY_NUM%	Код уровня важности события. Возможные значения: • 1 – **Информационное сообщение**. • 2 – **Предупреждение**. • 3 – **Сбой**. • 4 – **Критическое**.
%HOST_IP%	IP-адрес устройства, на котором произошло событие.
%HOST_CONN_IP%	IP-адрес соединения устройства, на котором произошло событие.

Пример:

Для уведомления о событии используется исполняемый файл (например, script1.bat), внутри которого запускается другой исполняемый файл (например, script2.bat) с подстановочным параметром %COMPUTER%. При возникновении события на устройстве администратора будет запущен файл script1.bat, который, в свою очередь, запустит файл script2.bat с параметром %COMPUTER%. В результате администратор получит имя устройства, на котором произошло событие.

Объявления "Лаборатории Касперского"

В этом разделе описано, как использовать, настраивать и отключать объявления "Лаборатории Касперского".

Об объявлениях "Лаборатории Касперского"

Раздел Объявления "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"** предоставляет информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. Kaspersky Security Center периодически обновляет информацию в разделе, удаляет устаревшие объявления и добавляет новую информацию.

Kaspersky Security Center показывает только те объявления "Лаборатории Касперского", которые относятся к текущему подключенному Серверу администрирования и программам "Лаборатории Касперского", установленным на управляемых устройствах этого Сервера администрирования. Объявления отображаются индивидуально для любого типа Сервера администрирования – главного, подчиненного или виртуального.

Для получения объявлений "Лаборатории Касперского" Сервер администрирования должен иметь подключение к интернету.

Объявления включают информацию следующих типов:

- Объявления, связанные с безопасностью.

  Объявления, связанные с безопасностью, предназначены для того, чтобы программы "Лаборатории Касперского", установленные в вашей сети, были в актуальном состоянии и были полностью функциональными. В объявлениях может содержаться информация о критических обновлениях для программ "Лаборатории Касперского", исправлениях для обнаруженных уязвимостей и способах устранения других проблем в программах "Лаборатории Касперского". По умолчанию объявления, связанные с безопасностью, включены. Если вы не хотите получать объявления, вы можете отключить эту функцию.

  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, которое вы принимаете при установке Сервера администрирования Kaspersky Security Center.

- Рекламные объявления.

  Рекламные объявления включают информацию о специальных предложениях для ваших программ "Лаборатории Касперского", рекламу и новости "Лаборатории Касперского". Рекламные объявления по умолчанию выключены. Вы получаете этот тип объявлений только в том случае, если вы включили Kaspersky Security Network (KSN). Вы можете выключить рекламные объявления, выключив KSN.

Чтобы показывать вам только актуальную информацию, которая может быть полезна для защиты ваших сетевых устройств и выполнения повседневных задач, Kaspersky Security Center отправляет данные на облачные серверы "Лаборатории Касперского" и получает соответствующие объявления. Данные, которые могут быть отправлены на серверы, описан в разделе "Обрабатываемые данные" Положения о KSN.

Информация разделена на следующие категории по важности:

1. Критическая информация.
2. Важная новость.
3. Предупреждение.
4. Информационное сообщение.

При появлении новой информации в разделе Объявления "Лаборатории Касперского" программа Kaspersky Security Center 14 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", включая категории объявлений, которые вы хотите просматривать, и место отображения метки уведомления. Если вы не хотите получать объявления, вы можете отключить эту функцию.

Настройка параметров объявлений "Лаборатории Касперского"

В разделе Объявления "Лаборатории Касперского" вы можете указать параметры объявлений "Лаборатории Касперского", включая категории объявлений, которые вы хотите просматривать, и где отображать метку уведомления.

Чтобы настроить объявления "Лаборатории Касперского":

1. В главном окне программы перейдите в раздел **Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**.
2. Перейдите по ссылке **Параметры**.

   Откроется окно объявлений "Лаборатории Касперского".
3. Задайте следующие параметры:
   - Выберите уровень важности объявлений, которые вы хотите просматривать. Объявления других категорий отображаться не будут.
   - Выберите расположение, где вы хотите видеть метку уведомления. Метка может отображаться во всех разделах консоли или в разделе **Мониторинг и отчеты** и его подразделах.
4. Нажмите на кнопку **ОК**.

   Параметры объявлений "Лаборатории Касперского" настроены.

Выключение объявлений "Лаборатории Касперского"

Раздел объявлений "Лаборатории Касперского" (**Мониторинг и отчеты** → **Объявления "Лаборатории Касперского"**) предоставляет информацию о вашей версии Kaspersky Security Center и управляемых программах, установленных на управляемых устройствах. Если вы не хотите получать объявления "Лаборатории Касперского", вы можете отключить эту функцию.

Чтобы отключить объявления "Лаборатории Касперского":

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

   Откроется окно свойств Сервера администрирования.
2. На закладке **Общие** выберите раздел **Объявления "Лаборатории Касперского"**.
3. Переведите переключатель в положение **Объявления, связанные с безопасностью**, выключено.
4. Нажмите на кнопку **Сохранить**.

   Объявления "Лаборатории Касперского" выключены.

Экспорт событий в SIEM-системы

В этом разделе описывается, как настроить экспорт событий в SIEM-системы.

Настройка экспорта событий в SIEM-системы

Kaspersky Security Center Linux 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 Linux:

- Узнайте больше о методах экспорта событий.
- Убедитесь, что у вас есть значения системных параметров.

> 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 Linux**

  Инструкции: Настройка экспорта событий в SIEM-системе.

- **Выбор событий, которые вы хотите экспортировать в SIEM-систему**

  Отметьте события, которые вы хотите экспортировать в SIEM-систему. Отметьте общие события, которые возникают во всех управляемых программах "Лаборатории Касперского". Затем можно отметить события для экспорта для определенной управляемой программы.

- **Настройка экспорта событий в SIEM-систему**

  Экспортировать события можно следующими способами:

  - Укажите протоколы TCP/IP, UDP или TLS over TCP.
  - Использование экспорта событий напрямую из базы данных Kaspersky Security Center. В базе данных Kaspersky Security Center представлен набор публичных представлений; вы можете найти описание этих общедоступных представлений в документе klakdb.chm.

Результаты

После настройки экспорта событий в SIEM-систему вы можете просматривать результаты экспорта, если вы выбрали события, которые хотите экспортировать.

Предварительные условия

Развернуть все | Свернуть все

При настройке автоматического экспорта событий в Kaspersky Security Center Linux необходимо указать некоторые параметры SIEM-системы. Рекомендуется уточнить эти параметры заранее, чтобы подготовиться к настройке Kaspersky Security Center Linux.

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 Linux и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center Linux и настройках приемника в SIEM-системе.

- **Протокол**

  Протокол, используемый для передачи сообщений из Kaspersky Security Center Linux в SIEM-систему. Это значение необходимо указать в настройках Kaspersky Security Center Linux и настройках приемника в SIEM-системе.

Об экспорте событий

Kaspersky Security Center Linux позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Информация о событиях сохраняется в базе данных Сервера администрирования.

Вы можете использовать экспорт событий в централизованных системах, работающих с вопросами безопасности на организационном и техническом уровнях, обеспечивающих мониторинг систем безопасности и консолидирующих данные из различных решений. К ним относятся SIEM-системы, обеспечивающие анализ предупреждений систем безопасности и событий сетевого аппаратного обеспечения и программ в режиме реального времени, а также центры управления безопасностью (Security Operation Center, SOC).

SIEM-системы получают данные из многих источников, включая сети, системы безопасности, серверы, базы данных и программы. Они также обеспечивают функцию объединения обработанных данных, что не позволит вам пропустить критические события. Кроме того, эти системы выполняют автоматический анализ связанных событий и сигналов тревоги для уведомления администраторов о вопросах системы безопасности, требующих незамедлительного решения. Уведомления могут отображаться на панели индикаторов или рассылаться по сторонним каналам, например, по электронной почте.

В процедуре экспорта событий из Kaspersky Security Center Linux во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center Linux и получатель событий – SIEM-система. Для успешного экспорта событий необходимо выполнить настройки и в используемой SIEM-системе, и в Консоли администрирования Kaspersky Security Center Linux. Последовательность настройки не имеет значения: Вы можете либо сначала настроить отправку событий в Kaspersky Security Center Linux, 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, можно передавать любые события, произошедшие на Сервере администрирования Kaspersky Security Center и в программах "Лаборатории Касперского", установленных на управляемых устройствах. При экспорте событий с использованием формата 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 Linux. 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 Linux во внешние SIEM-системы участвуют две стороны: отправитель событий – Kaspersky Security Center Linux и получатель событий – SIEM-система. Экспорт событий необходимо настроить в используемой SIEM-системе и в Kaspersky Security Center Linux.

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 Linux. 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 Linux для передачи событий.

- **Порт**

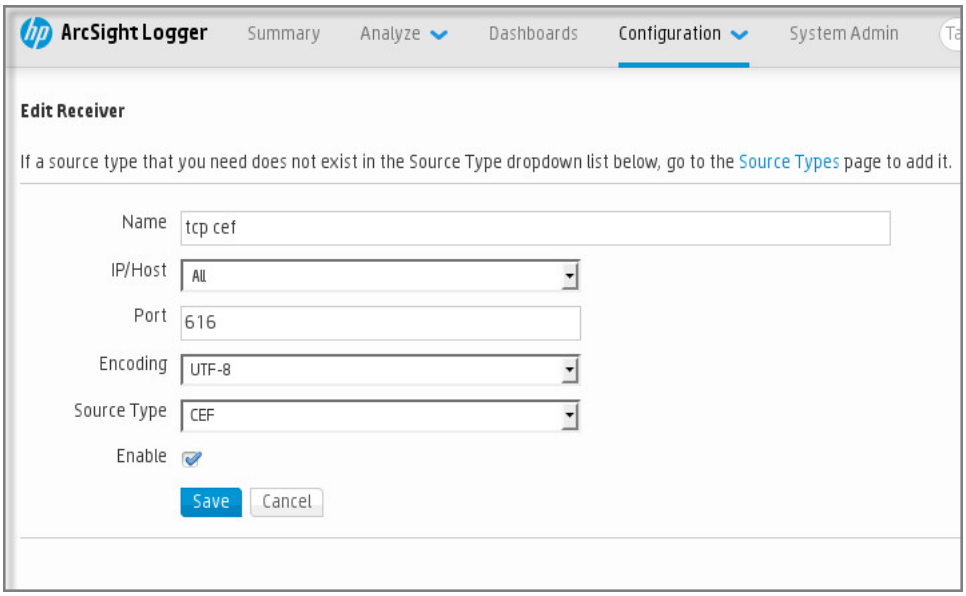
  Укажите номер порта для подключения к Kaspersky Security Center Linux. Этот порт должен совпадать с портом, который вы указываете в Kaspersky Security Center Linux при настройке экспорта событий в SIEM-систему.

- **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.



Настройка приемника в ArcSight

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, параметры. В результате SIEM-система имеет возможность выполнять обработку событий, полученных из Kaspersky Security Center Linux, таким образом, чтобы они сохранялись в базе данных SIEM-системы.

Выбор событий для экспорта в SIEM-системы в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.

- Выбор событий для управляемой программы. Если вы выбираете экспортируемые события для управляемой программы, установленной на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

О выборе событий для экспорта в SIEM-систему в формате Syslog

После включения автоматического экспорта событий необходимо выбрать, какие события будут экспортироваться во внешнюю SIEM-систему.

Вы можете настроить экспорт событий в формате Syslog во внешнюю систему на основе одного из следующих условий:

- Выбор общих событий. Если вы выберите экспортируемые события в политике, в свойствах события или в свойствах Сервера администрирования, то в SIEM-систему будут переданы выбранные события, которые произошли во всех программах, управляемых данной политикой. Если экспортируемые события были выбраны в политике, вам не удастся их переопределить для отдельной программы, управляемой этой политикой.

- Выбор событий для управляемой программы. Если вы выбираете экспортируемые события для управляемой программы, установленной на управляемых устройствах, то в SIEM-систему будут переданы только события, которые произошли в этой программе.

Выбор событий программ "Лаборатории Касперского" для экспорта в формате Syslog

Если вы хотите выполнить экспорт событий, произошедших в определенной управляемой программе, установленной на управляемых устройствах, выберите события для экспорта политике программы. В этом случае отмеченные события экспортируются со всех устройств, входящих в область действия политики.

Чтобы отметить события для экспорта для определенной управляемой программы:

1. В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**.

2. Выберите политику программы, для которой нужно отметить события.

   Откроется окно свойств политики.

3. Перейти в раздел **Настройка событий**.
4. Установите флажки рядом с событиями, которые требуется экспортировать в SIEM-систему.
5. Нажмите на кнопку **Отметить для экспорта в SIEM-систему по протоколу Syslog**.

> Также вы можете выбрать событие для экспорта в SIEM-систему в разделе **Регистрация событий**, который открывается по ссылке на событие.

6. Флажок (✓) появляется в графе **Syslog** для события или событий, которые вы отметили для экспорта в SIEM-систему.
7. Нажмите на кнопку **Сохранить**.

Отмеченные события из управляемой программы готовы к экспорту в SIEM-систему.

Вы можете отметить, какие события экспортировать в SIEM-систему для конкретного управляемого устройства. В случае, если ранее экспортируемые события были выбраны в политике программы, вам не удастся переопределить выбранные события для управляемого устройства.

Чтобы выбрать события для управляемого устройства:

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

   Отобразится список управляемых устройств.
2. Перейдите по ссылке с названием требуемого устройства в списке управляемых устройств.

   Откроется окно свойств выбранного устройства.
3. Перейти в раздел **Программы**.
4. Перейдите по ссылке с названием требуемой программы в списке программ.
5. Перейти 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.

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:
   - Нажмите на значок параметров (🔧) рядом с именем требуемого Сервера администрирования.
   - В главном окне программы перейдите в раздел **Устройства → Политики и профили политик**, а затем перейдите по ссылке политики.
2. В открывшемся окне перейдите на закладку **Настройка событий**.
3. Нажмите на 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.

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.

Об экспорте событий в формате Syslog

Используя формат Syslog можно выполнять экспорт в SIEM-системы событий, произошедших на Сервере администрирования и в других программах "Лаборатории Касперского", установленных на управляемых устройствах.

Syslog – это стандартный протокол регистрации сообщений. Этот протокол позволяет разделить программное обеспечение, генерирующее сообщения, систему, в которой хранятся сообщения, и программное обеспечение, выполняющее анализ и отчетность по сообщениям. Каждому сообщению присваивается код устройства, указывающий тип программного обеспечения, с помощью которого было создано сообщение, и уровень важности.

Формат Syslog определяется документами Request for Comments (RFC), опубликованными Internet Engineering Task Force. Стандарт RFC 5424 используется для экспорта событий из Kaspersky Security Center Linux во внешние системы.

В Kaspersky Security Center Linux 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 Linux таким образом, чтобы выполнялась отправка событий в SIEM-систему. Отправка событий из Kaspersky Security Center Linux 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.

Настройка Kaspersky Security Center Linux для экспорта событий в SIEM-систему

Развернуть все | Свернуть все

Для экспорта событий в SIEM-систему необходимо настроить процесс экспорта в Kaspersky Security Center Linux.

Чтобы настроить экспорт в SIEM-системы из Kaspersky Security Center 14 Web Console:

1. В раскрывающемся списке **Параметры консоли** выберите **Интеграция**.

   Откроется окно **Параметры консоли**.

2. Выберите закладку **Интеграция**.

3. На закладке **Интеграция** выберите раздел **SIEM**.

4. Перейдите по ссылке **Параметры**.

   Откроется раздел **Параметры экспорта**.

5. Укажите параметры в разделе **Параметры экспорта**:

   - **Адрес сервера SIEM-системы**

     Адрес сервера, на котором установлена используемая SIEM-система. Это значение необходимо уточнить в настройках SIEM-системы.

   - **Порт SIEM-системы**

     Номер порта, по которому будет установлено соединение между Kaspersky Security Center Linux и сервером SIEM-системы. Это значение необходимо указать в настройках Kaspersky Security Center Linux и настройках приемника в SIEM-системе.

   - **Протокол**

     Выберите протокол передачи сообщений в SIEM-систему. Вы можете выбрать протокол TCP, UDP или TLS over TCP.

     Укажите следующие параметры TLS, если вы выбираете TLS over TCP:

     - **Аутентификация Сервера**

       В поле **Аутентификация Сервера** можно выбрать значения **Доверенные сертификаты** или же **Отпечатки SHA**:

       - **Доверенные сертификаты**. Вы можете получить полную цепочку сертификатов (включая корневой сертификат) от доверенного центра сертификации (CA) и загрузить его в Kaspersky Security Center Linux. Kaspersky Security Center Linux проверяет, подписана ли цепочка сертификатов SIEM-системы также доверенным центром сертификации или нет.

         Чтобы добавить доверенный сертификат, нажмите на кнопку **Выбрать файл центра сертификации** и загрузите сертификат.

- **Отпечатки SHA**. Вы можете указать отпечатки SHA1 всей цепочки сертификатов SIEM-системы (включая корневой сертификат) в Kaspersky Security Center. Чтобы добавить отпечаток SHA1, введите его в поле **Отпечаток** и нажмите на кнопку **Добавить**.

  С помощью **Добавить проверку подлинности клиента** вы можете сгенерировать сертификат для аутентификации Kaspersky Security Center. Таким образом, вы будете использовать самоподписанный сертификат, выпущенный Kaspersky Security Center. В этом случае для аутентификации сервера SIEM-системы можно использовать как доверенный сертификат, так и отпечаток SHA.

- **Добавить имя субъекта/альтернативное имя субъекта**

  Имя субъекта – это доменное имя, для которого получен сертификат. Kaspersky Security Center Linux не может подключиться к серверу SIEM-системы, если доменное имя сервера SIEM-системы не совпадает с именем субъекта сертификата сервера SIEM-системы. Однако сервер SIEM-системы может изменить свое доменное имя, если имя изменилось в сертификате. В этом случае вы можете указать имена субъектов в поле **Добавить имя субъекта/альтернативное имя субъекта**. Если какое-либо из указанных имен субъектов совпадает с именем субъекта сертификата SIEM-системы, Kaspersky Security Center Linux проверяет сертификат сервера SIEM-системы.

- **Добавить проверку подлинности клиента**

  Для аутентификации клиента вы можете вставить свой сертификат или сгенерировать его в Kaspersky Security Center.

  - **Вставить сертификат**. 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:

    - **X.509-сертификат PEM**. Загрузите файл с сертификатом в поле **Файл с сертификатом** и файл с закрытым ключом в поле **Файл с ключом**. Оба файла не зависят друг от друга. Порядок загрузки файлов не имеет значения. Когда оба файла будут загружены, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

    - **X.509-сертификат PKCS12**. Загрузите один файл, содержащий сертификат и его закрытый ключ, в поле **Файл с сертификатом**. Когда файл будет загружен, укажите пароль для расшифровки закрытого ключа в поле **Проверка пароля или сертификата**. Пароль может иметь пустое значение, если закрытый ключ не зашифрован.

  - **Сгенерировать ключ**. Вы можете сгенерировать самоподписанный сертификат в Kaspersky Security Center. В результате Kaspersky Security Center Linux сохраняет сгенерированный самоподписанный сертификат, и вы можете передать публичную часть сертификата или SHA1-отпечаток в SIEM-систему.

6. 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**.

7. Переключите параметр в положение **Автоматически экспортировать события в базу SIEM-системы Включено**.

8. Нажмите на кнопку **Сохранить**.

Экспорт в SIEM-систему настроен. Если вы настроили получение событий в SIEM-системе, Сервер администрирования экспортирует отмеченные события в SIEM-систему. Если вы зададите дату начала экспорта, Сервер администрирования также экспортирует отмеченные события, хранящиеся в базе данных Сервера администрирования, начиная с указанной даты.

Экспорт событий напрямую из базы данных

Вы можете извлекать события напрямую из базы данных Kaspersky Security Center, не используя интерфейс Kaspersky Security Center Linux. 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 Linux 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 Linux, например, устройствам, программам, пользователям. Вы можете использовать эту информацию при создании запросов.

В этом разделе приведены инструкции по выполнению SQL-запроса с помощью утилиты klsql2, а также пример такого запроса.

Вы также можете использовать любые другие программы для работы с базами данных для создания SQL-запросов и представлений баз данных. Информация о том, как посмотреть параметры подключения к базе данных Kaspersky Security Center Linux, например, имя инстанса и имя базы данных, приведена в соответствующем разделе.

Выполнение SQL-запроса с помощью утилиты klsql2

В этой статье приведены инструкции по использованию утилиты klsql2, а также по выполнению SQL-запроса с использованием этой утилиты. При выполнении SQL-запроса с помощью утилиты klsql2 нет необходимости в явном виде указывать имя и параметры доступа для базы данных, поскольку запрос обращается напрямую к публичным представлениям Kaspersky Security Center Linux.

Чтобы использовать утилиту klsql2:

1. Перейдите в папку установки Сервера администрирования Kaspersky Security Center Linux. По умолчанию задан путь /opt/kaspersky/ksc64/sbin.
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 Linux, в командной строке введите следующую команду для выполнения SQL-запроса из файла src.sql и сохранения результатов в файл result.xml:
   ```
   sudo ./klsql2 -i src.sql -o result.xml
   ```
6. Откройте созданный файл result.xml и посмотрите результаты выполнения SQL-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 SQL-запрос и сохранить результаты в файл.

Пример SQL-запроса, созданного с помощью утилиты klsql2

В этом разделе приведен пример SQL-запроса, выполненного с помощью утилиты klsql2.

Следующий пример показывает, как получить список событий, зарегистрированных на устройствах пользователей за последние 7 дней, и отсортировать их по времени возникновения. Сначала отображаются самые последние события.

Пример:

```
SELECT

/* идентификатор события */
e.nId,

/* время возникновения события */
e.tmRiseTime,

/* внутреннее имя типа события  */
e.strEventType,

/* отображаемое имя события */
e.wstrEventTypeDisplayName,

/* отображаемое описание события */
e.wstrDescription,

/* имя группы, в которую входит устройство */
e.wstrGroupName,

/* отображаемое имя устройства, на котором произошло событие  */
h.wstrDisplayName,
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

/* IP-адрес устройства, на котором произошло событие */
CAST(((h.nIp) & 255) AS varchar(4)) as strIp
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
```

Просмотр имени базы данных Kaspersky Security Center Linux

Для доступа к базе данных Kaspersky Security Center Linux с помощью 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 Linux:

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.

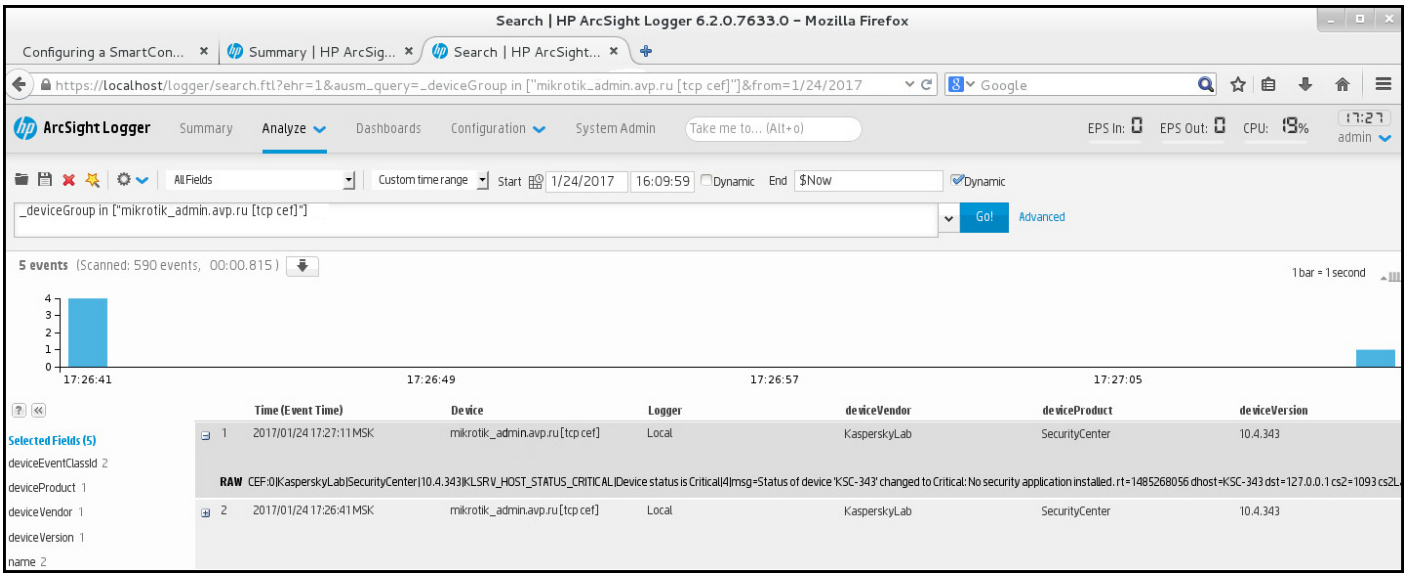
Просмотр результатов экспорта

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 Linux 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 Linux 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.



Пример событий

Выборки устройств

Выборки устройств – это инструмент для фильтрации устройств в соответствии с заданными условиями. Вы можете использовать выборки устройств, чтобы управлять несколькими устройствами: например, для просмотра отчетов только о выбранных устройствах или для перемещения всех этих устройств в другую группу администрирования.

Kaspersky Security Center предоставляет широкий диапазон *предопределенных выборок устройств* (например, **Устройства со статусом "Критический"**, **Защита выключена**, **Обнаружены активные угрозы**). Предопределенные выборки нельзя удалить. Вы можете также создавать и настраивать дополнительные *пользовательские выборки событий*.

В пользовательских выборках вы можете задать область поиска и выбрать все устройства, управляемые устройства или нераспределенные устройства. Параметры поиска задаются в условиях. В выборках устройств вы можете создать несколько условий с различными параметрами поиска. Например, вы можете создать два условия и задать различные IP-диапазоны в каждом из них. Если задано несколько условий, в выборку устройств попадут устройства, которые удовлетворяют любому из условий. Напротив, параметры поиска в одном условии накладываются друг на друга. Если в условии выборки заданы IP-диапазон и название установленной программы, то в выборку устройств попадут только те устройства, на которых одновременно установлена указанная программа и их IP-адреса входят в указанный диапазон.

Просмотр списка устройств из выборки устройств

Kaspersky Security Center позволяет просматривать список устройств из выборки устройств.

Чтобы просмотреть список устройств из выборки устройств:

1. В главном окне программы перейдите в раздел **Устройства → Выборки устройств** или в раздел **Обнаружение устройств и развертывание → Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Вы можете группировать и фильтровать данные таблицы устройств следующим образом:
   - Нажмите на значок параметров (⚙) и выберите столбцы для отображения в таблице.
   - Нажмите на значок фильтрации (), укажите и примените критерий фильтрации в открывшемся меню.

     Отобразится отфильтрованная таблица устройств.

Вы можете выбрать одно или несколько устройств в выборке устройств и нажать на кнопку **Новая задача**, чтобы создать задачу, которая будет применена к этим устройствам.

Чтобы переместить выбранные устройства из выборки устройств в другую группу администрирования, нажмите на кнопку **Переместить в группу** и выберите целевую группу администрирования.

Создание выборки устройств

Чтобы создать выборку устройств:

1. В главном окне программы перейдите в раздел **Устройства → Выборки устройств**.

   Отобразится страница со списком выборок устройств.
2. Нажмите на кнопку **Добавить**.

   Откроется окно **Параметры выборки устройств**.
3. Введите имя новой выборки.
4. Укажите группу, содержащую устройства, которые будут включены в выборку устройств:
   - **Искать любые устройства** – поиск устройств, соответствующих критериям выборки, в группах **Управляемые устройства** или **Нераспределенные устройства**.
   - **Искать управляемые устройства** – поиск устройств, соответствующих критериям выборки, в группе **Управляемые устройства**.
   - **Искать нераспределенные устройства** – поиск устройств, соответствующих критериям выборки, в группе **Нераспределенные устройства**.

   Вы можете установить флажок **Включать данные подчиненных Серверов администрирования**, чтобы включить поиск устройств, отвечающих критериям выборки, на подчиненных Серверах администрирования.
5. Нажмите на кнопку **Добавить**.
6. В открывшемся окне укажите условия, которые должны быть выполнены для включения устройств в эту выборку и нажмите на кнопку **OK**.
7. Нажмите на кнопку **Сохранить**.

Выборка устройств создана и добавлена в список выборок устройств.

Настройка выборки устройств

Развернуть все | Свернуть все

Чтобы настроить параметры выборки устройств:

1. В главном окне программы перейдите в раздел **Устройства → Выборки устройств**.

   Отобразится страница со списком выборок устройств.
2. Выберите соответствующую пользовательскую выборку устройств и нажмите на кнопку **Свойства**.

   Откроется окно **Параметры выборки устройств**.
3. На закладке **Общие** перейдите по ссылке **Новое условие**.
4. Укажите условия, которые должны быть выполнены, чтобы устройство было включено в эту выборку.
5. Нажмите на кнопку **Сохранить**.

Параметры применены и сохранены.

Ниже описаны параметры условий отнесения устройств к выборке. Условия сочетаются по логическому "или": в выборку попадают устройства, удовлетворяющие хотя бы одному из представленных условий.

Общие

В разделе **Общие** можно изменить имя условия выборки и указать, необходимо ли инвертировать это условие:

Инвертировать условие выборки

Если этот параметр включен, заданное условие выборки будет инвертировано. В выборку попадут все устройства, не соответствующие условию.

По умолчанию параметр выключен.

Инфраструктура сети

В разделе **Сеть** можно настроить критерии включения устройств в выборку на основании их сетевых данных:

- **Имя устройства**

  Имя устройства в сети Windows (NetBIOS-имя) или IPv4-адрес или IPv6-адрес.

- **Windows-домен**

  Отображаются все устройства, входящие в указанную рабочую группу.

- **Группа администрирования**

  Будут отображаться устройства, входящие в указанную группу администрирования.

- **Описание**

  Текст, который содержится в окне свойств устройства: в поле **Описание** раздела **Общие**.

  Для описания текста в поле **Описание** допустимо использовать следующие символы:

  - Внутри одного слова:
    - *****. Заменяет любую строку длиной 0 и более символов.

    Пример:

    Для описания слов **Сервер**, **Серверный** или Серверная можно использовать строку **Сервер***.

    - **?.** Заменяет любой один символ.

    Пример:

    Для описания таких фраз, как **SUSE Linux корпоративный сервер 12** или же **SUSE Linux корпоративный сервер 15**, можно ввести **SUSE Linux Enterprise Server 1?**.

    Звездочка (*****) или вопросительный знак (**?**) не могут использоваться как первый символ в описании текста.

  - Для связи нескольких слов:
    - Пробел. Отображает все устройства, описания которых содержат любое из перечисленных слов.

    Пример:

    Для описания фразы, содержащей слово **Подчиненный** или **Виртуальный** можно использовать строку **Подчиненный Виртуальный**.

    - **+.** При написании перед словом обозначает обязательное наличие слова в тексте.

    Пример:

    Для описания фразы, содержащей и слово **Подчиненный**, и слово **Виртуальный**, можно использовать строку **+Подчиненный+Виртуальный**.

- **-**. При написании перед словом обозначает обязательное отсутствие слова в тексте.

  Пример:

  Для описания фразы, в которой должно присутствовать слово **Подчиненный**, но должно отсутствовать слово **Виртуальный**, можно использовать строку **+Подчиненный-Виртуальный**.

- **"<фрагмент текста>"**. Фрагмент текста, заключенный в кавычки, должен полностью присутствовать в тексте.

  Пример:

  Для описания фразы, содержащей словосочетание **Подчиненный Сервер**, можно использовать строку **"Подчиненный Сервер"**.

- **IP-диапазон**

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

  По умолчанию параметр выключен.

- **Под управлением другого Сервера администрирования**

  Выберите одно из следующих значений:

  - **Да**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым другими Серверами администрирования. Эти Серверы отличаются от Сервера, на котором вы настраиваете правило перемещения устройств.
  - **Нет**. Правило перемещения устройств применяется только к клиентским устройствам, управляемым текущим Сервером администрирования.
  - **Значение не выбрано**. Условие не применяется.

В разделе **Active Directory** можно настроить критерии включения устройств в выборку на основании их данных Active Directory:

- **Устройство в подразделении Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из подразделения Active Directory, указанного в поле ввода.

  По умолчанию параметр выключен.

- **Включать дочерние подразделения**

  Если этот параметр включен, в выборку будут включаться устройства, входящие в дочерние подразделения указанной организационной единицы контроллера домена.

  По умолчанию параметр выключен.

- **Это устройство является членом группы Active Directory**

  Если этот параметр включен, в выборку будут включаться устройства из группы Active Directory, указанной в поле ввода.

  По умолчанию параметр выключен.

В разделе **Сетевая активность** можно настроить критерии включения устройств в выборку на основании их сетевой активности:

- **Является точкой распространения**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Да**. В выборку будут включены устройства, являющиеся точками распространения.
  - **Нет**. Устройства, являющиеся точками распространения, не будут включены в выборку.
  - **Значение не выбрано**. Критерий не применяется.

- **Не разрывать соединение с Сервером администрирования**

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:

  - **Включен**. Выборка будет включать устройства, для которых установлен флажок **Не разрывать соединение с Сервером администрирования**.

- **Выключен**. Выборка будет включать устройства, для которых снят флажок **Не разрывать соединение с Сервером администрирования**.
- **Значение не выбрано**. Критерий не применяется.

- Переключение профиля подключения

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:
  - **Да**. В выборку будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Нет**. В выборку не будут входить устройства, подключенные к Серверу администрирования в результате переключения профиля подключения.
  - **Значение не выбрано**. Критерий не применяется.

- Последнее подключение к Серверу администрирования

  С помощью этого флажка можно задать критерий поиска устройств по времени последнего соединения с Сервером администрирования.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее соединение установленного на клиентском устройстве Агента администрирования с Сервером администрирования. В выборку будут включены устройства, соответствующие установленному интервалу.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- Новые устройства, обнаруженные при опросе сети

  Поиск новых устройств, обнаруженных при опросе сети за последние несколько дней.

  Если этот параметр включен, то в выборку попадают только новые устройства, найденные в процессе обнаружения устройств за количество дней, которое указано в поле **Период обнаружения (сут)**.

  Если этот параметр выключен, то в выборку попадают все устройства, найденные в процессе обнаружения устройств.

  По умолчанию параметр выключен.

- Устройство в сети

  В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске:
  - **Да**. Программа включает в выборку устройства, которые видимы в сети в настоящий момент.
  - **Нет**. Программа включает в выборку устройства, которые не видимы в сети в настоящий момент.
  - **Значение не выбрано**. Критерий не применяется.

Статусы устройств

В разделе **Статус управляемых устройств** можно настроить критерии включения устройств в выборку по описанию статуса устройства от управляемой программы:

- Статус устройства

  Раскрывающийся список, в котором можно выбрать один из статусов устройства: *OK*, *Критический* или *Предупреждение*.

- Статус постоянной защиты

  Раскрывающийся список, в котором можно выбрать значение статуса задачи постоянной защиты. Устройства с указанным статусом постоянной защиты будут включаться в выборку.

- Описание статуса устройства

  В этом поле можно установить флажки для условий, при соблюдении которых устройству будет присваиваться выбранный статус: *OK*, *Критический* или *Предупреждение*.

В разделе **Статусы компонентов управляемых программ** можно настроить критерии включения устройств в выборку по статусам компонентов управляемых программ:

- Статус защиты данных от утечек

  Поиск устройств по статусу компонента защиты от утечки данных (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

- Статус защиты для серверов совместной работы

  Поиск устройств по статусу защиты для серверов совместной работы (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

- Статус антивирусной защиты почтовых серверов

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

- Статус Endpoint Sensor

  Поиск устройств по статусу компонента Endpoint Sensor (*Нет данных от устройства*, *Остановлена*, *Запускается*, *Приостановлена*, *Выполняется*, *Сбой*).

В разделе **Проблемы, связанные со статусом управляемых программ** можно настроить критерии включения устройств в выборку в соответствии со списком возможных проблем, обнаруженных управляемой программой. Если на устройстве существует хотя бы одна проблема, которую вы выбирали, устройство будет включено в выборку. Когда вы выбираете проблему, указанную для нескольких программ, у вас есть возможность автоматически выбрать эту проблему во всех списках.

Вы можете установить флажки для описаний статусов от управляемой программы, при получении которых устройства будут включаться в выборку. Когда вы выбираете статус, указанный для нескольких программ, у вас есть возможность автоматически выбирать этот статус во всех списках.

Сведения о системе

В разделе **Операционная система** можно настроить критерии включения устройств в выборку на основании установленной на них операционной системы.

- Тип платформы

  Если флажок установлен, в списке можно выбрать операционные системы. Устройства, на которых установлены указанные операционные системы, включаются в результаты поиска.

- Версия пакета обновления операционной системы

  В поле можно указать версию пакета установленной операционной системы (в формате *X.Y*), по наличию которой к устройству применяется правило перемещения. По умолчанию значения версии не заданы.

- Архитектура операционной системы

  В раскрывающемся списке можно выбрать архитектуру операционной системы, по наличию которой к устройству применяется правило перемещения (**Нет данных**, **x86**, **AMD64** или **IA64**). По умолчанию в списке не выбран ни один вариант, архитектура операционной системы не задана.

- Номер сборки операционной системы

  Этот параметр применим только для операционных систем Windows.

  Номер сборки операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний номер сборки. Вы также можете настроить поиск всех номеров сборки, кроме указанного.

- Номер выпуска операционной системы

  Этот параметр применим только для операционных систем Windows.

  Идентификатор выпуска операционной системы. Вы можете указать, должна ли выбранная операционная система иметь равный, более ранний или более поздний идентификатор выпуска. Вы также можете настроить поиск всех номеров идентификаторов выпуска, кроме указанного.

В разделе **Виртуальные машины** можно настроить критерии включения устройств в выборку в зависимости от того, являются эти устройства виртуальными машинами или частью Virtual Desktop Infrastructure:

- Является виртуальной машиной

  В раскрывающемся списке можно выбрать следующие элементы:
  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться виртуальными машинами.
  - **Да**. Искомые устройства должны являться виртуальными машинами.

- Тип виртуальной машины

  В раскрывающемся списке можно выбрать производителя виртуальной машины.

  Этот список доступен, если в раскрывающемся списке **Является виртуальной машиной** выбрано значение **Да** или **Неважно**.

- Часть Virtual Desktop Infrastructure

  В раскрывающемся списке можно выбрать следующие элементы:
  - **Не определено**.
  - **Нет**. Искомые устройства не должны являться частью Virtual Desktop Infrastructure.
  - **Да**. Искомые устройства должны являться частью Virtual Desktop Infrastructure (VDI).

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.

- Поставщик

  В раскрывающемся списке можно выбрать имя производителя оборудования. Все устройства с таким оборудованием включены в результат поиска.

  В поле поддерживается полнотекстовый поиск.

- Имя устройства

  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**

  Минимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Частота процессора (МГц) до**

  Максимальная тактовая частота процессора. Устройства с процессорами, соответствующими диапазону тактовой частоты, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора от**

  Минимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Количество виртуальных ядер процессора до**

  Максимальное количество виртуальных ядер CPU. Устройства с процессорами, соответствующими диапазону количества виртуальных ядер, указанному в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), от**

  Минимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем жесткого диска (ГБ), до**

  Максимальный объем жесткого диска устройства. Устройства с жесткими дисками, соответствующими диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) от**

  Минимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

- **Объем оперативной памяти (МБ) до**

  Максимальный объем оперативной памяти устройства. Устройства с оперативной памятью, соответствующей диапазону значений в полях ввода (включительно), будут включены в состав выборки.

Информация о программах сторонних производителей

В разделе **Реестр программ** можно настроить критерии включения устройств в выборку в зависимости от того, какие программы на них установлены:

- **Название программы**

  Раскрывающийся список, в котором можно выбрать программу. Устройства, на которых установлена указанная программа, будут включены в выборку.

- **Версия программы**

  Поле ввода, в котором указывается версия выбранной программы.

- **Поставщик**

  Раскрывающийся список, в котором можно выбрать производителя установленной на устройстве программы.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Искать по обновлению**

  Если этот параметр включен, поиск будет выполняться по данным об обновлении программ, установленных на искомых устройствах. После установки этого флажка вместо полей **Название программы**, **Версия программы** и **Статус программы** будут отображаться поля **Имя обновления**, **Версия обновления** и **Статус** соответственно.

  По умолчанию параметр выключен.

- **Название несовместимой программы безопасности**

  Раскрывающийся список, в котором можно выбрать программы безопасности сторонних производителей. Во время поиска устройства, на которых установлена выбранная программа, будут включены в выборку.

- **Тег программы**

  В раскрывающемся списке можно выбрать тег программы. Все устройства, на которых установлены программы, имеющие выбранный тег в описании, включаются в выборку устройств.

- **Применить к устройствам без выбранных тегов**

  Если параметр включен, в выборку будут включены устройства, в описании которых нет выбранных тегов.

  Если этот параметр выключен, критерий не применяется.

  По умолчанию параметр выключен.

Информация о программах "Лаборатории Касперского"

В разделе **Программы "Лаборатории Касперского"** можно настроить критерии включения устройств в выборку на основании выбранной управляемой программы:

- **Название программы**

В раскрывающемся списке можно выбрать критерий включения устройств в состав выборки при поиске по наименованию программы "Лаборатории Касперского".

В списке представлены названия только тех программ, для которых на рабочем месте администратора установлены плагины управления.

Если программа не выбрана, то критерий не применяется.

- **Версия программы**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по номеру версии программы "Лаборатории Касперского".

  Если номер версии не указан, то критерий не применяется.

- **Название критического обновления**

  В поле ввода можно указать критерий включения устройств в состав выборки при поиске по установленному для программы наименованию или номеру пакета обновления.

  Если поле не заполнено, то критерий не применяется.

- **Статус программы**

  Раскрывающийся список, в котором можно выбрать статус программы (*Установлена*, *Не установлена*). Устройства, на которых указанная программа установлена или не установлена, в зависимости от выбранного статуса, будут включены в выборку.

- **Последнее обновление модулей программы**

  С помощью этого параметра можно задать критерий поиска устройств по времени последнего обновления модулей программ, установленных на устройствах.

  Если флажок установлен, в полях ввода можно указать значения интервала (дата и время), в течение которого было выполнено последнее обновление модулей программ, установленных на устройствах.

  Если флажок снят, то критерий не применяется.

  По умолчанию флажок снят.

- **Устройство находится под управлением Kaspersky Security Center 14**

  В раскрывающемся списке можно включить в состав выборки устройства, которые находятся под управлением Kaspersky Security Center Linux:

  - **Да**. Программа включает в выборку устройства, которые находятся под управлением Kaspersky Security Center Linux.
  - **Нет**. Программа включает в выборку устройства, которые не находятся под управлением Kaspersky Security Center Linux.
  - **Значение не выбрано**. Критерий не применяется.

- **Программа безопасности установлена**

  В раскрывающемся списке можно включить в состав выборки устройства, на которых установлена программа безопасности:

  - **Да**. Программа включает в выборку устройства, на которых установлена программа безопасности.
  - **Нет**. Программа включает в выборку устройства, на которых не установлена программа безопасности.
  - **Значение не выбрано**. Критерий не применяется.

В разделе **Антивирусная защита** можно настроить критерии включения устройств в выборку по состоянию защиты:

- **Дата выпуска баз**

  Если этот параметр выбран, поиск клиентских устройств выполняется по дате выпуска антивирусных баз. В полях ввода можно задать временной интервал, на основании которого будет выполняться поиск.

  По умолчанию параметр выключен.

- **Количество записей в базах**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству записей в базе. В полях ввода можно задать нижнее и верхнее значения количества записей антивирусной базы.

  По умолчанию параметр выключен.

- **Последняя проверка**

  Если этот параметр включен, поиск клиентских устройств выполняется по времени последнего поиска вирусов. В полях ввода можно указать интервал, в течение которого антивирусная проверка выполнялась в последний раз.

  По умолчанию параметр выключен.

- **Обнаружены угрозы**

  Если этот параметр включен, поиск клиентских устройств выполняется по количеству найденных вирусов. В полях ввода можно задать нижнее и верхнее значения количества найденных вирусов.

  По умолчанию параметр выключен.

Подраздел **Компоненты программы** содержит список компонентов тех программ, которые имеют соответствующие плагины управления, установленные в Kaspersky Security Center 14 Web Console.

В разделе **Компоненты программы** вы можете задать критерий для включения устройств в выборку в соответствии с номерами версий компонентов, относящихся к выбранной программе:

- **Статус**

  Поиск устройств в соответствии со статусом компонента, отправленным управляемой программой на Сервер администрирования. Вы можете выбрать один из следующих статусов: *Нет данных от устройства*, *Остановлен*, *Приостановлено*, *Запускается*, *Выполняется*, *Сбой*, *Не установлен*, *Не поддерживается лицензией*. Если выбранный компонент программы, установленный на управляемом устройстве, имеет указанный статус, устройство входит в выборку устройств.

  Статусы, отправленные программами:

  - *Остановлено* – компонент отключен и в данный момент не работает.
  - *Приостановлено* – компонент приостановлен, например, после того, как пользователь приостановил защиту в управляемой программе.
  - *Запускается* – компонент в настоящее время находится в процессе инициализации.
  - *Выполняется* – компонент включен и работает правильно.
  - *Сбой* – во время выполнения операции компонента произошла ошибка.
  - *Не установлено* – пользователь не выбрал компонент для установки во время выборочной установки программы.
  - *Не поддерживается лицензией* – лицензия не распространяется на выбранный компонент.

  В отличие от других статусов, статус *Нет данных от устройства* не отправляется управляемой программой. Этот параметр показывает, что программы не имеют информации о выбранном статусе компонента. Например, это может произойти, если выбранный компонент не принадлежит ни одной из программ, установленных на устройстве, или устройство выключено.

- **Версия**

  Поиск устройств в соответствии с номером версии компонента, который вы выбрали в списке. Вы можете ввести номер версии, например, `3.4.1.0`, а затем указать, должен ли выбранный компонент иметь равную, более раннюю или более позднюю версию. Также вы можете настроить поиск по всем версиям компонента, кроме указанной.

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**

  Если этот параметр включен, вы можете выбрать учетную запись пользователя, для которой настроили критерий. В результаты поиска включаются устройства, на которых последний вход в систему выполнялся выбранным пользователем.

- **Пользователь, уже выполнявший вход в систему**

  Если этот параметр включен, при нажатии на кнопку **Обзор** можно указать учетную запись пользователя. В результаты поиска включаются устройства, на которых указанный пользователь когда-либо выполнял вход в систему.

Экспорт списка устройств из выборки устройств

Kaspersky Security Center позволяет сохранять информацию об этих устройствах из выборки устройств в файл CSV или TXT.

Чтобы экспортировать список устройств из выборки устройств в файл:

1. Откройте таблицу с устройствами из выборки устройств.
2. Вы можете экспортировать информацию об устройствах из таблицы одним из следующих способов:

   - Экспортировать выбранные устройства.

     Установите флажки рядом с требуемыми устройствами и нажмите на кнопку **Экспортировать строки в файл формата CSV** или **Экспортировать строки в файл формата TXT** в зависимости от формата, который вы хотите экспортировать. Вся информация о выбранных устройствах, включенных в таблицу, будет экспортирована в файл TXT или CSV.

   - Экспортировать все устройства, отображаемые на текущей странице.

     Нажмите на кнопку **Экспортировать строки в файл формата CSV** или **Экспортировать строки в файл формата TXT**, в зависимости от формата, который вы хотите экспортировать. Вам не нужно выбирать устройства из таблицы. Вся информация об устройствах, отображаемая на текущей странице, будет экспортирована в файл TXT.

Обратите внимание, если вы отфильтровали таблицу устройств, в файл CSV или TXT будут экспортированы только отфильтрованные данные отображаемых столбцов.

Удаление устройств из групп администрирования в выборке

При работе с выборкой устройств вы можете удалять устройства из групп администрирования прямо в выборке, не переходя к работе с группами администрирования, из которых требуется удалить устройства.

Чтобы удалить устройства из групп администрирования:

1. В главном окне программы перейдите в раздел **Устройства** → **Выборки устройств** или **Обнаружение устройств и развертывание** → **Выборки устройств**.
2. В списке выборок нажмите на имя выборки устройств.

   На странице отображается таблица с информацией об устройствах, включенных в выборку устройств.
3. Выберите устройства, которые вы хотите удалить и нажмите на кнопку **Удалить**.

   В результате выбранные устройства будут удалены из групп администрирования, в которые они входили.

Изменение языка интерфейса Kaspersky Security Center 14 Web Console

Вы можете выбрать язык интерфейса Kaspersky Security Center 14 Web Console.

Чтобы изменить язык интерфейса:

1. В главном меню перейдите в параметры своей учетной записи и выберите **Язык**.
2. Выберите один из поддерживаемых языков локализации.

Справочное руководство API

Справочное руководство по Kaspersky Security Center OpenAPI предназначено для решения следующих задач:

- Автоматизация и настройка. Вы можете автоматизировать задачи, которые, возможно, не хотите выполнять вручную. Например, как администратор вы можете использовать Kaspersky Security Center OpenAPI для создания и запуска сценариев, которые упростят разработку структуры групп администрирования и поддержат ее в актуальном состоянии.
- Пользовательская разработка. Используя OpenAPI, вы можете разработать клиентскую программу.

Вы можете использовать поле поиска в правой части экрана, чтобы найти нужную информацию в справочном руководстве OpenAPI.

Справочное руководство OpenAPI

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", запускать задачи в Kaspersky Security Center или назначать точки распространения. Вы можете запускать примеры как есть или создавать собственные сценарии на их основе.

Чтобы вызвать методы OpenAPI и запустить сценарии:

1. Загрузите архив KlAkOAPI.tar.gz . 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.

   Вызывать методы OpenAPI, запускать примеры и свои сценарии можно только на устройствах, на которых установлены Сервер администрирования и пакет KlAkOAPI.

Сопоставление пользовательских сценариев и примеров методов Kaspersky Security Center OpenAPI

Пример	Назначение примера	Сценарий
Журнал событий KlAkParams	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
Создание и удаление иерархии "главный/подчиненный"	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 и удаление иерархии Серверов администрирования
Создайте иерархию группы со структурой на основе	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем загрузить файл со списком сетей на свой компьютер.	Настройка точек распространения и шлюзов соединений

подразделения Active Directory.		
Создайте иерархию группы со структурой на основе кешированного подразделения Active Directory.	Вы можете подключиться к главному Серверу администрирования, загрузить с него необходимый лицензионный ключ и передать этот ключ на все подчиненные Серверы администрирования, входящие в иерархию.	Лицензирование управляемых программ
Загрузите файлы списка сетей с помощью шлюза соединения на указанное устройство	Вы можете создать разные отчеты. 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
Установить лицензионный ключ, хранящийся в хранилище главного Сервера администрирования, на подчиненные Серверы администрирования	Вы можете подключиться к Агенту администрирования на нужном устройстве, используя шлюз соединения, а затем запустить необходимую задачу.	Запуск задачи вручную
Создайте отчет об эффективных правах пользователей	Вы можете назначить управляемые устройства точками распространения (ранее они назывались "агенты обновлений").	Обновление баз и программ "Лаборатории Касперского"
Запустить задачу для устройства.	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
Создание IP-подсетей на основе сайта и служб Active Directory	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
Регистрация точек распространения для устройств в группе	Вы можете создать задачу. Укажите в примере следующие параметры задачи: • Тип. • Способ запуска. • Имя. • Группа устройств, для которой будет использоваться задача. По умолчанию в примере создается задача типа "Показать сообщение". Вы можете запустить эту задачу для всех управляемых устройств Сервера администрирования. При необходимости вы можете указать свои параметры задачи.	Создание задачи
Перечисление всех групп	Вы можете получить список всех активных лицензионных ключей для программ "Лаборатории Касперского", установленных на управляемых устройствах Сервера администрирования. Список содержит подробные сведения о каждом лицензионном ключе, такие как имя, тип или срок действия.	Просмотр информации об используемых лицензионных ключах
Перечисление задач, запрос статистики задач и запуск задач	Вы можете создать учетную запись для дальнейшей работы.	Добавление учетной записи внутреннего пользователя
Создание и запуск задачи	Вы можете создать категорию программ с требуемыми параметрами.	Создание пополняемой вручную категории программ

Перечисление лицензионных ключей	Вы можете использовать класс SrvView для запроса подробной информации с Сервера администрирования. Например, вы можете получить список пользователей, используя этот пример.	Управление пользователями и ролями пользователей

Программы, взаимодействующие с Kaspersky Security Center через OpenAPI

Некоторые программы взаимодействуют с Kaspersky Security Center через OpenAPI. К таким программам относятся, например, Kaspersky Anti Targeted Attack Platform или Kaspersky Security для виртуальных сред. Это также может быть пользовательская клиентская программа, разработанная вами на основе OpenAPI.

Программы, взаимодействующие с Kaspersky Security Center через OpenAPI, подключаются к Серверу администрирования. Если вы настроили список разрешенных IP-адресов для подключения к Серверу администрирования, добавьте IP-адреса устройств, на которых установлены программы, использующие Kaspersky Security Center OpenAPI. Чтобы узнать, работает ли используемая вами программа с OpenAPI, обратитесь к справке этой программы.

Лучшие практики для поставщиков услуг

В этой справке вы найдете информацию о настройке и использовании Kaspersky Security Center Linux.

Документ содержит рекомендации по развертыванию, настройке и использованию программы, а также способы решения типичных проблем, возникающих при работе программы.

Планирование развертывания Kaspersky Security Center Linux

Планируя развертывание компонентов Kaspersky Security Center Linux в сети организации, следует принимать во внимание размер и масштаб проекта, а также следующие факторы:

- общего количества устройств;
- количество MSP-клиентов.

Один Сервер администрирования может обслуживать не более чем 50 000 устройств. Если общее количество устройств в сети организации превышает 50 000, следует разместить на стороне MSP несколько Серверов администрирования, объединенных в иерархию для удобства централизованного управления.

На одном Сервере администрирования может быть создано до 500 виртуальных Серверов, следовательно, на каждые 500 MSP-клиентов необходим отдельный Сервер администрирования.

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;
- для задания желательных значений полей сертификата;
- для обеспечения желаемой криптографической стойкости сертификата.

Предоставление доступа к Серверу администрирования из интернета

Для того чтобы устройства, размещенные в сети клиента, могли обращаться к Серверу администрирования через интернет, необходимо сделать доступными следующие порты Сервера администрирования:

- 13000 TCP – порт TLS Сервера администрирования, к данному порту подключаются Агенты администрирования, размещенные в сети клиента;
- 8061 TCP – порт HTTPS для публикации автономных пакетов средствами Kaspersky Security Center 14 Web Console;
- 8060 TCP – порт HTTP для публикации автономных пакетов средствами Kaspersky Security Center 14 Web Console;
- 13292 TCP – данный TLS порт нужен, только если требуется управлять мобильными устройствами.
- 8080 TCP – порт HTTPS для Kaspersky Security Center 14 Web Console.

Типовая конфигурация Kaspersky Security Center Linux

На серверах MSP размещен один или несколько Серверов администрирования. Количество Серверов может быть выбрано как исходя из наличия доступного аппаратного обеспечения, так и в зависимости от количества обслуживаемых MSP-клиентов или же общего количества управляемых устройств.

Один Сервер администрирования может обслуживать до 50 000 устройств. Нужно учесть возможность увеличения количества управляемых устройств в ближайшем будущем: может оказаться желательным подключение несколько меньшего количества устройств к одному Серверу администрирования.

На одном Сервере администрирования может быть создано до 500 виртуальных Серверов, следовательно, на каждые 500 MSP-клиентов необходим отдельный Сервер администрирования.

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: выполнять поиск устройств, создавать выборки устройств, создавать отчеты.

На каждом виртуальном Сервере, соответствующем MSP-клиенту, следует назначить по одной или по несколько точек распространения. Так как связь между MSP-клиентами и Сервером администрирования 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".

Если в сети MSP-клиента часть устройств не имеет прямого доступа в интернет, то точки распространения следует переключить в режим шлюза соединений. В таком случае Агенты администрирования на устройствах в сети MSP-клиента будут подключаться (с целью синхронизации) к Серверу администрирования не напрямую, а через шлюз.

Поскольку Сервер администрирования, скорее всего, не сможет опрашивать сеть MSP-клиента, 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 сети MSP-клиента. Для решения этой проблемы стоит включить в свойствах устройств, являющихся точками распространения и работающих в режиме шлюза соединения, режим постоянного соединения с Сервером администрирования (параметр **Не разрывать соединение с Сервером администрирования**). Режим постоянного соединения доступен, если общее количество точек распространения не превышает 300.

MSP-клиент может захотеть управлять Android- и iOS-устройствами сотрудников. Сервер администрирования управляет мобильными устройствами по протоколу TLS и TCP-порту 13292.

О точках распространения

Устройство с установленным Агентом администрирования может быть использовано в качестве точки распространения. В этом режиме Агент администрирования может выполнять следующие функции:

- Передачу файлов на клиентские устройства, включая:
  - Базы и модули программ "Лаборатории Касперского".

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

Размещение точек распространения в сети организации преследует следующие цели:

- Уменьшить нагрузку на Сервер администрирования в случае, если источником обновлений служит Сервер администрирования.
- Оптимизировать интернет-трафик, так как в этом случае каждому устройству в сети MSP-клиента не придется обращаться за обновлениями к серверам "Лаборатории Касперского" или к Серверу администрирования.
- Предоставить Серверу администрирования доступ к устройствам за NAT (по отношению к Серверу администрирования) сети MSP-клиента 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.

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, выполняющее роль точки распространения, не обязано принадлежать группе администрирования, на которую оно назначено.

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. Этот режим полезен в сценариях, когда между устройствами с Агентом администрирования и Сервером администрирования невозможно прямое соединение.

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

Иерархия Серверов администрирования

У MSP может быть более одного Сервера администрирования. Администрировать несколько разрозненных Серверов неудобно, поэтому целесообразно объединять их в иерархию.

В иерархии Сервер администрирования Kaspersky Security Center Linux может работать только как подчиненный Сервер под управлением главного Сервера администрирования Kaspersky Security Center на базе Windows или Kaspersky Security Center Cloud Console.

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

- Подчиненный Сервер наследует с главного Сервера политики и задачи, устраняется дублирование параметров.
- Выборки устройств на главном Сервере могут включать в себя устройства с подчиненных Серверов.
- Отчеты на главном Сервере могут включать в себя данные (в том числе и детальные) с подчиненных Серверов.

Главный Сервер администрирования получает данные только от не виртуальных 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.

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. Для максимальной взаимной изоляции MSP-клиентов рекомендуется выбирать виртуальные Серверы администрирования, которые будут использоваться для определенных задач. Кроме того, создание виртуального Сервера для каждого MSP-клиента позволяет предоставить клиентам базовые возможности по администрированию своей сети посредством Kaspersky Security Center 14 Web Console.

Виртуальные Серверы во многом подобны подчиненным Серверам администрирования, однако имеют следующие отличия:

- виртуальный Сервер не имеет большинства глобальных параметров и собственных TCP-портов;
- у виртуального Сервера не может быть подчиненных Серверов;
- у виртуального Сервера не может быть собственных виртуальных Серверов;
- на физическом Сервере администрирования видны устройства, группы, события и объекты с управляемых устройств (элементы карантина, реестра программ и прочее) всех его виртуальных Серверов;
- виртуальный Сервер может сканировать сеть только посредством подключенных к нему точек распространения.

Развертывание и первоначальная настройка

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

- Сервер администрирования – центральный компонент, ответственный за управление устройствами организации и хранение данных в СУБД.
- Kaspersky Security Center 14 Web Console – веб-интерфейс Сервера администрирования для выполнения простейших операций. Этот компонент можно установить на любое устройство, удовлетворяющее требованиям к аппаратному и программному обеспечению.
- Агент администрирования – служит для управления установленной на устройстве программой безопасности, а также для получения информации об устройстве. Агенты администрирования устанавливаются на устройства организации.

Развертывание Kaspersky Security Center Linux в сети организации осуществляется следующим образом:

- установка Сервера администрирования;
- установка Kaspersky Security Center 14 Web Console;
- установка Агента администрирования и программы безопасности на устройства организации.

Рекомендации по установке Сервера администрирования

В этом разделе содержатся рекомендации, касающиеся установки Сервера администрирования. В разделе также содержатся сценарии использования папки общего доступа на устройстве с Сервером администрирования для развертывания Агента администрирования на клиентских устройствах.

Создание учетных записей для служб Сервера администрирования на отказоустойчивом кластере

Прежде чем начать развертывание Kaspersky Security Center на отказоустойчивом кластере, вам нужно создать учетные записи для служб Kaspersky Security Center.

Для этого на активном узле, пассивном узле и файловом сервере выполните следующие шаги:

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.

Выбор СУБД

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

Рекомендации и ограничения СУБД

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

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

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

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

Если вы установите MySQL, MariaDB, PostgreSQL или Postgres Pro используйте рекомендуемые параметры, чтобы обеспечить правильную работу СУБД.

Если вы используете СУБД PostgreSQL, MariaDB или MySQL, на вкладке **События** может отображаться неполный список событий для выбранного клиентского устройства. Это происходит, когда СУБД хранит очень большое количество событий. Вы можете увеличить количество отображаемых событий, выполнив одно из следующих действий:

- Удалить ненужные события.
- Сократить срок хранения ненужных событий.

Чтобы увидеть полный список событий, зарегистрированных на Сервере администрирования для устройства, используйте Отчеты.

Указание адреса Сервера администрирования

При установке Сервера администрирования необходимо задать DNS-имя или статический IP-адрес Сервера администрирования. Этот адрес по умолчанию используется при создании инсталляционных пакетов Агента администрирования. В дальнейшем адрес Сервера администрирования можно будет изменить средствами Kaspersky Security Center 14 Web Console, однако при этом он не изменится автоматически в уже созданных инсталляционных пакетах Агента администрирования.

Развертывание Агента администрирования и программ безопасности

Для управления устройствами в организации и для их защиты от угроз безопасности, вам нужно установить Агент администрирования и программу безопасности "Лаборатории Касперского" на каждое устройство.

Подробнее о развертывании защиты см. раздел Развертывание Агента администрирования и программ безопасности.

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).

Настройка защиты в сети организации-клиента

После завершения установки Сервера администрирования запускается программа Kaspersky Security Center 14 Web Console, которая предлагает выполнить первоначальную настройку с помощью мастера. Во время работы мастера первоначальной настройки в корневой группе администрирования создаются следующие политики и задачи:

- политика Kaspersky Endpoint Security;
- групповая задача обновления Kaspersky Endpoint Security;
- групповая задача проверки устройства Kaspersky Endpoint Security;
- политика Агента администрирования;
- задача поиска уязвимостей (задача Агента администрирования);
- задача установки обновлений и закрытия уязвимостей (задача Агента администрирования).

Политики и задачи создаются с параметрами по умолчанию, которые могут оказаться неоптимальными или даже непригодными для данной организации. Поэтому следует просмотреть свойства созданных объектов и, в случае необходимости, внести изменения вручную.

В этом разделе содержится информация о ручной настройке политик, задач и других параметров Сервера администрирования, а также информация о точке распространения, построении структуры групп администрирования, иерархии задач и других настройках.

Ручная настройка политики Kaspersky Endpoint Security

Этот раздел содержит рекомендации по настройке параметров политики Kaspersky Endpoint Security, которую создает мастер первоначальной настройки. Вы можете выполнить настройку в окне свойств политики.

При изменении параметров, помните, что вы можете заблокировать или разблокировать параметр, чтобы запретить или разрешить изменение его значения на рабочей станции.

Настройка политики в разделе Продвинутая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Продвинутая защита** можно настроить использование Kaspersky Security Network для Kaspersky Endpoint Security для Windows. Можно также настроить модули Kaspersky Endpoint Security для Windows, такие как Анализ поведения, Защита от эксплойтов, Предотвращение вторжений и Откат вредоносных действий.

В подразделе **Kaspersky Security Network** рекомендуется включить параметр **Kaspersky Security Network**. Использование этого параметра поможет перераспределить и оптимизировать трафик сети. Если параметр **Kaspersky Security Network** выключен, вы можете включить прямое использование серверов KSN.

Настройка политики в разделе Базовая защита

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security для Windows.

В разделе **Базовая защита** окна свойств политики рекомендуется указать дополнительные параметры в подразделах **Сетевой экран** и **Защита от файловых угроз**.

Подраздел **Сетевой экран** содержит параметры, позволяющие контролировать сетевую активность программ на клиентских устройствах. Клиентское устройство использует сеть, которой присвоен один из следующих статусов: общедоступная, локальная или доверенная. В зависимости от состояния сети Kaspersky Endpoint Security может разрешить или запретить сетевую активность на устройстве. Когда вы добавляете новую сеть в свою организацию, вы должны присвоить ей соответствующий сетевой статус. Например, если клиентским устройством является ноутбук, рекомендуется, чтобы это устройство использовало общедоступную или доверенную сеть, так как ноутбук не всегда подключен к локальной сети. В подразделе **Сетевой экран** можно проверить, правильно ли вы присвоили статусы используемым в вашей организации сетям.

Чтобы проверить список сетей:

1. В свойствах политики перейдите в раздел **Базовая защита** → **Сетевой экран**.

2. В блоке **Доступные сети** нажмите на кнопку **Настройки**.

3. В открывшемся окне **Сетевой экран** перейдите на вкладку **Сети** для просмотра списка сетей.

В подразделе **Защита от файловых угроз** можно отключить проверку сетевых дисков. Проверка сетевых дисков может создавать значительную нагрузку на сетевые диски. Целесообразнее осуществлять проверку непосредственно на файловых серверах.

Чтобы выключить проверку сетевых дисков:

1. В свойствах политики перейдите в раздел **Базовая защита → Защита от файловых угроз**.

2. В блоке **Уровень безопасности** нажмите на кнопку **Настройки**.

3. В открывшемся окне **Защита от файловых угроз** на вкладке **Общие** снимите флажок **Все сетевые диски**.

Настройка политики в разделе Дополнительные параметры

Полное описание параметров этого раздела приведено в документации Kaspersky Endpoint Security.

Ниже описаны действия по дополнительной настройке, которые рекомендуется выполнить в окне свойств политики Kaspersky Endpoint Security в разделе **Общие параметры**.

Раздел Дополнительные параметры, подраздел Отчеты и хранилища

В разделе **Передача данных на Сервер администрирования**, обратите внимание на флажок **О запускаемых программах**. Если этот флажок установлен, в базе данных Сервера администрирования сохраняется информация о всех версиях всех программных модулей на устройствах в сети организации. Указанная информация может занимать значительный объем в базе данных Kaspersky Security Center Linux (десятки гигабайтов). Поэтому, если в политике верхнего уровня по-прежнему установлен флажок **О запускаемых программах**, его необходимо снять.

Раздел Дополнительные параметры, подраздел Интерфейс

Если управление защитой от угроз в сети организации необходимо выполнять централизованно через Консоль администрирования, нужно выключить отображение пользовательского интерфейса Kaspersky Endpoint Security на рабочих станциях (сняв флажок **Отображать интерфейс программы** в разделе **Взаимодействие с пользователем**) и включить защиту паролем (установив **флажок Включить защиту паролем** в разделе **Защита паролем**).

Настройка политики в разделе Настройка событий

В разделе **Настройка событий** следует выключить сохранение на Сервере администрирования всех событий, за исключением перечисленных ниже:

- На вкладке **Критическое**:
  - *Автозапуск приложения выключен*
  - *Доступ запрещен*
  - *Запуск приложения запрещен*
  - *Лечение невозможно*
  - *Нарушено Лицензионное соглашение*
  - *Не удалось загрузить модуль шифрования*
  - *Невозможен запуск двух задач одновременно*
  - *Обнаружена активная угроза. Требуется запуск процедуры лечения активного заражения*
  - *Обнаружена сетевая атака*
  - *Обновлены не все компоненты*
  - *Ошибка активации*
  - *Ошибка активации портативного режима*
  - *Ошибка взаимодействия с Kaspersky Security Center*
  - *Ошибка деактивации портативного режима*

- *Ошибка изменения состава компонентов приложения*
- *Ошибка применения правил шифрования / расшифровки файлов*
- *Политика не может быть применена*
- *Процесс завершен*
- *Сетевая активность запрещена*

- На вкладке **Отказ функционирования**: *Ошибка в настройках задачи. Настройки задачи не применены*
- На вкладке **Предупреждение**:
  - *Самозащита приложения выключена*
  - *Некорректный резервный ключ*
  - *Пользователь отказался от политики шифрования*
- На вкладке **Информационное**: *Запуск приложения запрещен в тестовом режиме*.

Ручная настройка групповой задачи обновления Kaspersky Endpoint Security

Если источником обновлений является Сервер администрирования, то для групповых задач обновления Kaspersky Endpoint Security оптимальным и рекомендуемым является расписание **При загрузке обновлений в хранилище** при установленном флажке **Использовать автоматическое определение случайного интервала между запусками задачи**.

Если для каждой точки распространения будет создана локальная задача загрузки обновлений в хранилище с серверов "Лаборатории Касперского", то для групповой задачи обновления Kaspersky Endpoint Security оптимальным и рекомендуемым будет периодический запуск по расписанию. Значение периода автономизации следует в этом случае установить в 1 час.

Ручная настройка групповой задачи проверки устройства Kaspersky Endpoint Security

Мастер первоначальной настройки создает групповую задачу проверки устройства. 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.

Настройка расписания задачи Поиск уязвимостей и требуемых обновлений

Мастер первоначальной настройки создает для Агента администрирования групповую задачу *Поиск уязвимостей и требуемых обновлений*. По умолчанию для задачи выбрано расписание **Запускать по вторникам в 19:00** с автоматической рандомизацией и установлен флажок **Запускать пропущенные задачи**.

Если регламент работы организации предусматривает выключение устройств в это время, то задача *Поиск уязвимостей и требуемых обновлений* будет запущена после включения устройства (в среду утром). Такое поведение может быть нежелательным, так как поиск уязвимостей может вызывать повышенную нагрузку на процессор и дисковую подсистему устройства. Следует настроить оптимальное расписание задачи исходя из принятого в организации регламента работы.

Ручная настройка групповой задачи установки обновлений и закрытия уязвимостей

Мастер первоначальной настройки создает для Агента администрирования групповую задачу установки обновлений и поиска уязвимостей. По умолчанию настроен запуск задачи ежедневно в 1:00 с автоматической рандомизацией, параметр **Запускать пропущенные задачи** выключен.

Если регламент работы организации предусматривает отключение устройств на ночь, то задача установки обновлений никогда не будет запущена. Следует задать оптимальное расписание задачи поиска уязвимостей исходя из принятого в организации регламента работы. Кроме того, следует учитывать, что в результате установки обновлений может потребоваться перезагрузка устройства.

Построение структуры групп администрирования и назначение точек распространения

Структура групп администрирования в Kaspersky Security Center Linux выполняет следующие функции:

- Задание области действия политик.

  Существует альтернативный способ применения нужных наборов параметров на устройствах с помощью профилей политик. В этом случае область действия политик устанавливается, например, с помощью тегов устройств или ролей пользователей.

- 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 MSP-клиента и топологии сетей можно выделить следующие типовые конфигурации структуры групп администрирования:

- один офис;
- множество небольших изолированных офисов.

Типовая конфигурация MSP-клиента: 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.

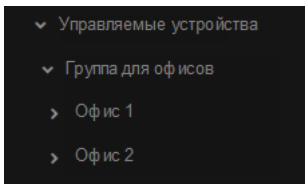
Возможны следующие способы построения структуры групп администрирования:

- 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 из Агентов администрирования будет подключаться к той точке распространения, маршрут к которой является самым коротким. Маршрут к точке распространения можно определить с помощью утилиты tracert или трассировкой маршрута.

Типовая конфигурация MSP-клиента: множество небольших изолированных офисов

Этой типовой конфигурации соответствует множество небольших удаленных офисов, возможно, связанных с главным офисом через интернет. Каждый из удаленных офисов находится за NAT, то есть подключение из одного удаленного офиса в другой невозможно – офисы изолированы друг от друга.

Конфигурацию следует обязательно отразить в структуре групп администрирования: для каждого из удаленных офисов следует создать отдельную группу администрирования (группы **Офис 1**, **Офис 2** на рисунке ниже).



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.

Иерархия политик, использование профилей политик

В этом разделе содержится информация об особенностях применения политик к устройствам в группах администрирования. В этом разделе также содержится информация о профилях политик.

Иерархия политик

В Kaspersky Security Center Linux политики предназначены для задания одинакового набора параметров на множестве устройств. Например, областью действия политики программы P, определенной для группы G, являются управляемые устройства с установленной программой P, размещенные в группе администрирования G и всех ее подгруппах, исключая те подгруппы, в свойствах которых снят флажок **Наследовать из родительской группы**.

Политика отличается от локальных параметров наличием "замков" (🔒) возле содержащихся в ней параметров. Установленный замок в свойствах политики означает, что соответствующий ему параметр (или группа параметров) должен, во-первых, быть использован при формировании эффективных параметров, во-вторых, должен быть записан в нижележащую политику.

Формирование на устройстве действующих параметров можно представить следующим образом: из политики берутся значения параметров с неустановленным замком, затем поверх них записываются значения локальных параметров, затем поверх полученных значений записываются взятые из политики значения параметров с установленным замком.

Политики одной и той же программы действуют друг на друга по иерархии групп администрирования: параметры с установленным замком из вышележащей политики переписывают одноименные параметры из нижележащей политики.

Существует особый вид политики – политика для автономных пользователей. Эта политика вступает в силу на устройстве, когда устройство переходит в автономный режим. Политики для автономных пользователей не действуют по иерархии групп администрирования на другие политики.

Профили политик

Применение политик к устройствам, исходя только из иерархии групп администрирования, во многих случаях неудобно. Может возникнуть необходимость создать несколько копий политики для разных групп администрирования и в дальнейшем вручную синхронизировать содержимое этих политик.

Чтобы помочь избежать подобных проблем, Kaspersky Security Center Linux поддерживает *профили политик*. 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 клиентском устройстве (компьютере, мобильном устройстве). При активации профиля изменяются параметры политики, действовавшие на устройстве до активации профиля. Эти параметры принимают значения, указанные в профиле.

Профили политик сейчас имеют следующие ограничения:

- в политике может быть не более 100 профилей;
- профиль политики не может содержать другие профили;
- профиль политики не может содержать параметры уведомлений.

Состав профиля

Профиль политики содержит следующие составные части:

- Имя. Профили с одинаковыми именами действуют друг на друга по иерархии групп администрирования с общим правилами.
- Подмножество параметров политики. В отличие от политики, где содержатся все параметры, в профиле присутствуют лишь те параметры, которые действительно нужны (на которых установлен замок).
- Условие активации – логическое выражение над свойствами устройства. Профиль активен (дополняет политику), только когда условие активации профиля становится истинным. В остальных случаях профиль неактивен и игнорируется. В логическом выражении могут участвовать следующие свойства устройства:
  - состояние автономного режима;
  - свойства сетевого окружения – имя активного правила подключения Агента администрирования;
  - наличие или отсутствие у устройства указанных тегов;
  - местоположение устройства в подразделении Active Directory: явное (устройство находится непосредственно в указанном подразделении) или неявное (устройство находится в подразделении, которое находится внутри указанного подразделения на любом уровне вложенности);
  - членство устройства в группе безопасности Active Directory (явное или неявное);
  - членство владельца устройства в группе безопасности Active Directory (явное или неявное).
- Флажок отключения профиля. Отключенные профили всегда игнорируются, условия их активации не проверяются на истинность.
- Приоритет профиля. Условия активации профилей независимы, поэтому одновременно могут активироваться сразу несколько профилей. Если активные профили содержат непересекающиеся наборы параметров, то никаких проблем не возникает. Но если два активных профиля

содержат разные значения одного и того же параметра, возникает неоднозначность. значение неоднозначной переменной будет взято из профиля с большим приоритетом (из того профиля, который располагается выше в списке профилей).

Поведение профилей при действии политик друг на друга по иерархии

Одноименные профили объединяются согласно правилам объединения политик. Профили верхней политики приоритетнее профилей нижней политики. Если в "верхней" политике запрещено изменение параметров (кнопка замок нажата), в "нижней" политике используются условия активации профиля из "верхней" политики. Если в "верхней" политике разрешено изменение параметров, то используются условия активации профиля из "нижней" политики.

Поскольку профиль политики может в условии активации содержать свойство **Устройство в автономном режиме**, профили полностью заменяют функциональность политик для автономных пользователей, которая в дальнейшем не будет поддерживаться.

Политика для автономных пользователей может содержать профили, но активация ее профилей может произойти не ранее, чем устройство перейдет в автономный режим.

Задачи

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

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

Задачи могут выполняться на Сервере администрирования и на устройствах.

Задачи, которые выполняются на Сервере администрирования:

- автоматическая рассылка отчетов;
- загрузка обновлений в хранилище Сервера администрирования;
- резервное копирование данных Сервера администрирования;
- обслуживание базы данных.

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 14 Web Console, но и пользователем удаленного устройства (например, в интерфейсе программы безопасности). Если локальная задача была изменена одновременно и администратором, и пользователем на управляемом устройстве, то вступят в силу изменения, внесенные администратором, как более приоритетные.

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

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

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

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

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

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

Результаты выполнения задач сохраняются в системном журнале событий и журнале событий Kaspersky Security Center как централизованно на Сервере администрирования, так и локально на каждом устройстве.

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

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. 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 Linux в явном виде, в разделе **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 снимите флажок **Перемещать только устройства, которые не входят ни в одну группу администрирования**.

Наличие правил перемещения, действующих на устройства, уже размещенные в группах администрирования, существенно увеличивает нагрузку на Сервер администрирования.

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 программ* 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 Linux (особенно в области прав доступа, событий и отчетов). Следует искать другое решение, например, использовать профили политик, задачи для выборок устройств, назначать Агенты администрирования согласно методике.

Категоризация программного обеспечения

Основным средством контроля запуска программ являются *категории "Лаборатории Касперского"* (далее также *KL-категории*). KL-категории облегчают администратору Kaspersky Security Center Linux работу по поддержанию категоризации ПО и минимизируют объем трафика, передаваемого на управляемые устройства.

Пользовательские категории следует создавать только для программ, не подпадающих ни под одну KL-категорию (например, для программ, разработанных на заказ). Пользовательские категории создаются на основе дистрибутива программы (MSI) или на основе папки с дистрибутивами.

В случае если имеется большая пополняемая коллекция программного обеспечения, не категоризированного при помощи KL-категорий, может быть целесообразным создать автоматически обновляемую категорию. Такая категория будет автоматически пополняться контрольными суммами исполняемых файлов при изменении папки с дистрибутивами.

Резервное копирование и восстановление параметров Сервера администрирования

Для резервного копирования параметров Сервера администрирования и используемой им базы данных предусмотрены задача резервного копирования и утилита klbackup. Резервная копия включает в себя все основные параметры и объекты Сервера администрирования: сертификаты Сервера администрирования, мастер-ключи шифрования дисков управляемых устройств, ключи для лицензий, структуру групп администрирования со всем содержимым, задачи, политики и так далее. Имея резервную копию, можно восстановить работу Сервера администрирования в кратчайшие сроки – от десятков минут до двух часов.

В случае отсутствия резервной копии сбой может привести к безвозвратной потере сертификатов и всех параметров Сервера администрирования. Это повлечет необходимость заново настраивать Kaspersky Security Center Linux, а также заново выполнять первоначальное развертывание Агента администрирования в сети организации. Кроме того, будут потеряны и мастер-ключи шифрования дисков управляемых устройств, что создаст риск безвозвратной потери зашифрованных данных на устройствах с Kaspersky Endpoint Security. Поэтому не следует отказываться от регулярного создания резервных копий Сервера администрирования с помощью штатной задачи резервного копирования.

Мастер первоначальной настройки программы создает задачу резервного копирования параметров Сервера администрирования с ежедневным запуском в четыре часа ночи. Резервные копии по умолчанию сохраняются в папке %ALLUSERSPROFILE%\Application Data\KasperskySC.

Поскольку резервная копия содержит важные данные, в задаче резервного копирования и в утилите klbackup предусмотрена защита резервных копий паролем. По умолчанию задача резервного копирования создается с пустым паролем. Следует обязательно задать пароль в свойствах задачи резервного копирования. Несоблюдение этого требования приведет к тому, что ключи сертификатов Сервера администрирования, ключи для лицензий и мастер-ключи шифрования дисков управляемых устройств окажутся незашифрованными.

Помимо регулярного резервного копирования, следует также создавать резервную копию перед всеми значимыми изменениями, в том числе перед обновлением Сервера администрирования до новой версии и перед установкой патчей Сервера администрирования.

Восстановление из резервной копии выполняется с помощью утилиты klbackup на только что установленном и работоспособном экземпляре Сервера администрирования той версии, для которой была сделана резервная копия (или более новой).

Экземпляр Сервера администрирования, на которую выполняется восстановление, должна использовать СУБД того же типа той же самой или более новой версии. Версия Сервера администрирования может быть той же самой (с аналогичным или более новым патчем) или более новой.

В этом разделе описаны типовые сценарии восстановления параметров и объектов Сервера администрирования.

Вышло из строя устройство с Сервером администрирования

Если в результате сбоя вышло из строя устройство с Сервером администрирования, рекомендуется выполнить следующие действия:

- Назначить новому Серверу тот же самый адрес: DNS-имя или статический IP-адрес, в зависимости от того, что было задано при развертывании Агентов администрирования.
- Установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
- Запустить утилиту klbackup и выполнить восстановление.

Повреждены параметры Сервера администрирования или база данных

Если Сервер администрирования стал неработоспособен в результате повреждения параметров или базы данных (например, из-за сбоя питания), рекомендуется использовать следующий сценарий восстановления:

1. Выполнить проверку файловой системы на пострадавшем устройстве.
2. Деинсталлировать неработоспособную версию Сервера администрирования.
3. Заново установить Сервер администрирования с использованием СУБД того же типа, той же или более новой версии. Можно установить ту же версию Сервера с тем же или более новым патчем, или более новую версию. После установки не следует выполнять первоначальную настройку с помощью мастера.
4. Запустите утилиту klbackup и выполните восстановление.

Недопустимо восстанавливать Сервер администрирования любым другим способом, кроме штатной утилиты klbackup.

Во всех случаях восстановления Сервера с помощью стороннего программного обеспечения неизбежно произойдет рассинхронизация данных на узлах распределенной программы Kaspersky Security Center Linux и, как следствие, неправильная работа программы.

О профилях соединения для автономных пользователей

При работе автономных пользователей, использующих ноутбуки (далее также "устройства"), может понадобиться изменить способ подключения к Серверу администрирования или переключиться между Серверами администрирования в зависимости от текущего положения устройства в сети.

Профили подключения поддерживаются только для устройств под управлением Windows и macOS.

Использование различных адресов одного и того же Сервера администрирования

Устройства с установленным Агентом администрирования могут в разные периоды времени подключаться к Серверу администрирования как из внутренней сети организации, так и из интернета. В этой ситуации может потребоваться, чтобы Агент администрирования использовал различные адреса для подключения к Серверу администрирования: внешний адрес Сервера при подключении из интернета и внутренний адрес Сервера при подключении из внутренней сети.

Для этого в свойствах политики Агента администрирования нужно добавить профиль для подключения к Серверу администрирования из интернета. Добавьте профиль в свойствах политики (раздел **Подключения**, вложенный раздел **Профили соединений**). В окне создания профиля необходимо выключить параметр **Использовать только для получения обновлений** и выбрать параметр **Синхронизировать параметры подключения с параметрами Сервера, указанными в этом профиле**. Если для доступа к Серверу администрирования используется шлюз соединений (например, в конфигурации Kaspersky Security Center Linux, описанной в разделе Доступ из интернета: Агент администрирования в качестве шлюза соединения в демилитаризованной зоне), в профиле подключения следует указать адрес шлюза соединения в соответствующем поле.

Переключение между Серверами администрирования в зависимости от текущей сети

Если в организации несколько офисов с различными Серверами администрирования и между ними перемещается часть устройств с установленным Агентом администрирования, то необходимо, чтобы Агент администрирования подключался к Серверу администрирования локальной сети того офиса, в котором находится устройство.

В этом случае в свойствах политики Агента администрирования следует создать профиль подключения к Серверу администрирования для каждого из офисов, за исключением домашнего офиса, в котором расположен исходный домашний Сервер администрирования. В профилях подключения следует указать адреса соответствующих Серверов администрирования и выбрать либо выключить параметр **Использовать только для получения обновлений**:

- выбрать параметр, если требуется, чтобы Агент администрирования синхронизировался с домашним Сервером администрирования, а локальный Сервер использовался только для загрузки обновлений;
- выключить параметр, если необходимо, чтобы Агент администрирования полностью управлялся локальным Сервером администрирования.

Далее необходимо настроить условия переключения на созданные профили: не менее одного условия для каждого из офисов, исключая "домашний офис". Смысл каждого такого условия заключается в обнаружении в сетевом окружении деталей, присущих одному из офисов. Если условие становится истинным, происходит активация соответствующего профиля. Если ни одно из условий не является истинным, Агент администрирования переключается на домашний Сервер администрирования.

Удаленный доступ к управляемым устройствам

Этот раздел содержит информацию об удаленном доступе к управляемым устройствам.

Использование параметра "Не разрывать соединение с Сервером администрирования" для обеспечения постоянной связи между управляемым устройством и Сервером администрирования

Если вы не используете push-серверы, Kaspersky Security Center Linux не обеспечивает постоянного соединения между управляемыми устройствами и Сервером администрирования. Агенты администрирования на управляемых устройствах периодически устанавливают соединение и синхронизируются с Сервером администрирования. Продолжительность периода такой синхронизации задается в политике Агента администрирования. Если требуется предварительная синхронизация, Сервер администрирования (или точка распространения, если она используется) отправляет подписанный сетевой пакет по IPv4- или IPv6-сети на UDP-порт Агента администрирования. Номер порта по умолчанию – 15000. Если подключение по UDP от Сервера администрирования к управляемому устройству невозможно, то синхронизация произойдет при очередном периодическом подключении Агента администрирования к Серверу в течение периода синхронизации.

Некоторые операции невозможно выполнить без предварительного соединения Агента администрирования с Сервером администрирования, например запуск и остановку локальных задач или получение статистики по управляемой программе. Чтобы решить эту проблему, если вы не используете push-серверы, вы можете использовать параметр **Не разрывать соединение с Сервером администрирования**, который обеспечивает постоянное соединения между управляемым устройством и Сервером администрирования.

Чтобы обеспечить постоянное соединение управляемого устройства с Сервером администрирования:

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

   Отобразится список управляемых устройств.

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

3. В окне свойств устройства в разделе **Общие** включите параметр **Не разрывать соединение с Сервером администрирования**.

Постоянное соединение установлено между управляемым устройством и Сервером администрирования.

Общее количество устройств, для которых выбран параметр **Не разрывать соединение с Сервером администрирования**, не должно превышать 300.

О проверке времени соединения устройства с Сервером администрирования

При выключении устройства Агент администрирования уведомляет Сервер администрирования о выключении. В Kaspersky Security Center 14 Web Console это устройство отображается как выключенное. Однако Агенту удается уведомить Сервер администрирования не во всех случаях. Поэтому Сервер администрирования для каждого устройства периодически анализирует атрибут **Соединение с Сервером администрирования** (значение атрибута отображается в Kaspersky Security Center 14 Web Console в свойствах устройства в разделе **Общие**) и сопоставляет его с периодом синхронизации из действующих параметров Агента администрирования. Если устройство не выходило на связь более чем три периода синхронизации, то такое устройство отмечается как выключенное.

О принудительной синхронизации

Несмотря на то что Kaspersky Security Center Linux автоматически синхронизирует состояние, параметры, задачи и политики для управляемых устройств, в отдельных случаях администратору нужно точно знать, что в текущий момент для определенного устройства синхронизация выполнена.

Окно свойств управляемого устройства содержит кнопку **Синхронизировать принудительно**. Когда Kaspersky Security Center 14 Linux выполняет команду синхронизации, Сервер администрирования пытается подключиться к устройству. Если эта попытка успешна, будет выполнена принудительная синхронизация. В противном случае принудительная синхронизация произойдет только после очередного выхода Агента администрирования на связь с Сервером.

Интеграция Kaspersky Security Center 14 Web Console с другими решениями "Лаборатории Касперского"

В этом разделе описывается, как настроить доступ из Kaspersky Security Center 14 Web Console к другой программе "Лаборатории Касперского", например Kaspersky Anti Targeted Attack (KATA) и Kaspersky Endpoint Detection and Response (KEDR). В этом разделе также описано как настроить экспорт в SIEM-системы.

Настройка доступа к веб-консоли KATA/KEDR

Kaspersky Anti Targeted Attack (KATA) и Kaspersky Endpoint Detection and Response (KEDR) это два функциональных блока программы Kaspersky Anti Targeted Attack Platform. Вы можете управлять этими функциональными блоками с помощью веб-консоли для Kaspersky Anti Targeted Attack Platform (веб-консоль KATA/KEDR). Если вы используете и Kaspersky Security Center 14 Web Console и веб-консоль KATA/KEDR, вы можете настроить доступ к веб-консоли KATA/KEDR напрямую через интерфейс программы Kaspersky Security Center 14 Web Console.

Чтобы настроить доступ к веб-консоли KATA/KEDR:

1. В главном окне программы нажмите **Параметры консоли** в верхней части экрана.
2. В раскрывающемся меню выберите пункт **Интеграция**.

   Откроется окно Параметры консоли.
3. На закладке **Интеграция** укажите веб-адрес веб-консоли KATA/KEDR в поле **Веб-адрес веб-консоли KATA/KEDR**.
4. Нажмите на кнопку **Сохранить**.

Раскрывающийся список **Расширенное управление** добавляется в верхнюю часть главного окна программы. Вы можете использовать это меню, чтоб открывать веб-консоль KATA/KEDR. После того, как вы нажмете **Advanced Cybersecurity**, в вашем браузере откроется новая закладка с указанным вами веб-адресом.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашего вопроса в документации Kaspersky Security Center Linux или других источниках информации о программе, обратитесь в Службу технической поддержки "Лаборатории Касперского". Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security Center Linux.

"Лаборатория Касперского" предоставляет поддержку Kaspersky Security Center Linux в течение ее жизненного цикла (см. страницу жизненного цикла программ). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с правилами предоставления технической поддержки .

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- посетить веб-сайт Службы технической поддержки;
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с портала Kaspersky CompanyAccount portal.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. На портале Kaspersky CompanyAccount можно отслеживать статус обработки электронных запросов специалистами "Лаборатории Касперского" и хранить историю электронных запросов.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Вы можете узнать больше о Kaspersky CompanyAccount на веб-сайте Службы технической поддержки.

Получение файлов дампа Сервера администрирования

Файлы дампа Сервера администрирования содержат всю информацию о процессах Сервера администрирования на определенный момент времени. Файлы дампа Сервера администрирования хранятся в директории /var/lib/systemd/coredump. Файлы дампа хранятся, пока используется Kaspersky Security Center, и удаляются безвозвратно при удалении приложения. Файлы дампа не отправляются в "Лабораторию Касперского" автоматически.

В случае сбоя Сервера администрирования вы можете обратиться в Службу технической поддержки "Лаборатории Касперского". Специалист Службы технической поддержки может попросить вас отправить файлы дампа Сервера администрирования для дальнейшего анализа в "Лаборатории Касперского".

Файлы дампа могут содержать персональные данные. Перед отправкой в "Лабораторию Касперского" рекомендуется защитить информацию от несанкционированного доступа.

Источники информации о программе

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

На странице Kaspersky Security Center вы можете получить общую информацию о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security Center в Базе знаний

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

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

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

Обсуждение программ "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.

На форуме пользователей вы можете просматривать опубликованные темы, добавлять свои комментарии, создавать новые темы для обсуждения.

Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в Службу технической поддержки.

Список ограничений

Kaspersky Security Center Linux имеет ряд ограничений, не критичных для работы программы:

- Если список содержит более 20 записей (в этом случае записи отображаются на нескольких страницах) и вы установили флажок **Выбрать все**, Web Console выбирает только те записи, которые отображаются на текущей странице.
- 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.
- Задача *Смена Сервера администрирования* не запускается автоматически после установки значения **Немедленно** в расписании задач и сохранения изменений.
- Если вы открываете Kaspersky Security Center 14 Web Console в разных браузерах и загружаете файл сертификата Сервера администрирования в окне свойств Сервера администрирования, загруженные файлы имеют разные имена.
- Ошибка возникает при попытке восстановить объект из хранилища **Резервное хранилище** (**Операции** → **Хранилища** → **Резервное хранилище**) или при отправке объекта в "Лабораторию Касперского".
- Параметры, заблокированные в родительской политике Kaspersky Endpoint Security для Linux, наследуются, но не блокируются в дочерних политиках.
- Информация об оборудовании, отправляемая с управляемого устройства на Сервер администрирования, может быть неполной; некоторое оборудование может быть не указано.
- Категория программ, которую вы добавили в компонент Контроль программ в политике Kaspersky Endpoint Security для Linux, может быть удалена.
- Управляемое устройство, имеющее более одного сетевого адаптера, отправляет Серверу администрирования информацию о MAC-адресе сетевого адаптера, отличного от того, который используется для подключения к Серверу администрирования.
- Если вы указали учетные записи пользователей в параметрах webConsoleAccount и managementServiceAccount файла ответов для установки Kaspersky Security Center 14 Web Console и эти учетные записи принадлежат к разным группам безопасности, Kaspersky Security Center 14 Web Console не работает после установки.
- В 64-разрядной версии Astra Linux пакет klnagent-astra нельзя обновить с помощью пакета klnagent64_14: старый пакет klnagent64-astra будет удален, а вместо обновления будет установлен новый пакет klnagent64, поэтому будет добавлен новый значок для устройства с пакетом klnagent64_14. Вы можете удалить старый значок для этого устройства.

Глоссарий

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.

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.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network – это решение, которое предоставляет пользователям устройств, с установленными программами "Лаборатории Касперского", доступ к базам данных Kaspersky Security Network и другим статистическим данным, без отправки данных со своих устройств в Kaspersky Security Network. Kaspersky Private Security Network предназначен для организаций, которые не могут участвовать в Kaspersky Security Network по одной из следующих причин:

- Устройства не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной сети (LAN) запрещена законом или корпоративными политиками безопасности.

Kaspersky 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.

Provisioning-профиль

Набор параметров для работы приложений на мобильных устройствах iOS. Provisioning-профиль содержит информацию о лицензии и привязан к конкретному приложению.

SSL

Протокол шифрования данных в локальных сетях и в интернете. SSL используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Агент администрирования

Компонент программы Kaspersky Security Center, осуществляющий взаимодействие между Сервером администрирования и программами "Лаборатории Касперского", установленными на конкретном сетевом узле (рабочей станции или сервере). Этот компонент является единым для всех программ, разработанных для систем Microsoft Windows. Для программ "Лаборатории Касперского" для операционных систем UNIX и подобных им и macOS существуют отдельные версии Агента администрирования.

Агент аутентификации

Интерфейс, позволяющий после шифрования загрузочного жесткого диска пройти процедуру аутентификации для доступа к зашифрованным жестким дискам и для загрузки операционной системы.

Административные права

Уровень прав и полномочий пользователя для администрирования объектов Exchange внутри организации Exchange.

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Администратор клиента

Сотрудник организации-клиента, который отвечает за обеспечение антивирусной защиты организации-клиента.

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.

Активный ключ

Ключ, используемый в текущий момент для работы программы.

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 защита сети повышается при использовании программ безопасности и сервисов, а также при наличии и соблюдении политики информационной безопасности в организации.

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.

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.

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).

Владелец устройства

Владелец устройства – это пользователь устройства, с которым администратор может контактировать в случае необходимости выполнить какие-либо работы с устройством.

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.

Восстановление

Перемещение оригинального объекта из карантина или резервного хранилища в папку его исходного расположения, где объект хранился до его помещения на карантин, лечения или удаления, либо другую папку, указанную пользователем.

Восстановление данных Сервера администрирования

Восстановление данных Сервера администрирования при помощи утилиты резервного копирования на основании информации, сохраненной в резервном хранилище. Утилита позволяет восстанавливать:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Группа администрирования

Набор устройств, объединенных в соответствии с выполняемыми функциями и устанавливаемым на них набором программ "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы могут входить другие группы. Для каждой из установленных в группе программ могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, определенная для группы администрирования и выполняемая на всех клиентских устройствах, входящих в состав этой группы администрирования.

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.

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.

Дополнительный (или резервный) лицензионный ключ

Ключ, подтверждающий право на использование программы, но не используемый в текущий момент.

Доступное обновление

Пакет обновлений модулей программы "Лаборатории Касперского", в состав которого включены набор срочных обновлений, собранных за некоторый период, и изменения в архитектуре программы.

Задача

Функции, выполняемые программой "Лаборатории Касперского", реализованы в виде задач, например: Постоянная защита файлов, Полная проверка устройства, Обновление баз.

Задача для набора устройств

Задача, определенная для набора клиентских устройств из произвольных групп администрирования и выполняемая на них.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" при помощи системы удаленного управления Kaspersky Security Center. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров соответствуют значениям параметров программы по умолчанию. Инсталляционный пакет создается на основании файлов с расширениями kpd и kud, входящих в состав дистрибутива программы.

Клиент Сервера администрирования (Клиентское устройство)

Устройство, сервер или рабочая станция, на котором установлен Агент администрирования и запущены управляемые программы "Лаборатории Касперского".

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 14 Web Console.

Конфигурационный профиль

Политика, содержащая набор параметров и ограничений для мобильного устройства iOS MDM.

Локальная задача

Задача, определенная и выполняющаяся на отдельном клиентском компьютере.

Локальная установка

Установка программы безопасности на устройство сети организации, которая предусматривает ручной запуск установки из дистрибутива программы безопасности или ручной запуск опубликованного инсталляционного пакета, предварительно загруженного на устройство.

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.

Непосредственное управление программой

Управление программой через локальный интерфейс.

Несовместимая программа

Антивирусная программа стороннего производителя или программа "Лаборатории Касперского", не поддерживающая управление через Kaspersky Security Center Linux.

Обновление

Процедура замены или добавления новых файлов (баз или программных модулей), получаемых с серверов обновлений "Лаборатории Касперского".

Общий сертификат

Сертификат, предназначенный для идентификации мобильного устройства пользователя.

Оператор Kaspersky Security Center

Пользователь, который ведет наблюдение за состоянием и работой системы защиты, управляемой при помощи Kaspersky Security Center.

Параметры задачи

Параметры работы программы, специфичные для каждого типа задачи.

Параметры программы

Параметры работы программы, общие для всех типов ее задач и отвечающие за работу программы в целом, например: параметры производительности программы, параметры ведения отчетов, параметры резервного хранилища.

Политика

Политика определяет параметры работы программы и доступ к настройке программы, установленной на устройствах группы администрирования. Для каждой программы требуется создать свою политику. Вы можете создать множество политик для программ, установленных на устройствах в каждой группе администрирования, но в пределах группы администрирования только одна политика может применяться единовременно к каждой программе.

Поставщик услуг антивирусной защиты

Организация, предоставляющая услуги антивирусной защиты сетей организации-клиента на основе решений "Лаборатории Касперского".

Профиль

Набор параметров поведения мобильных устройств Exchange при подключении к серверу Microsoft Exchange.

Рабочее место администратора

Устройство, на котором вы открываете Kaspersky Security Center 14 Web Console. Этот компонент, предоставляет интерфейс управления Kaspersky Security Center.

С рабочего места администратор управляет серверной частью Kaspersky Security Center. Используя рабочее место администратора, администратор выстраивает систему централизованной защиты сети организации, сформированной на базе программ "Лаборатории Касперского".

Резервное копирование данных Сервера администрирования

Копирование данных Сервера администрирования для резервного хранения и последующего восстановления, осуществляемое при помощи утилиты резервного копирования. Утилита позволяет сохранять:

- база данных Сервера администрирования (политики, задачи, параметры программ, сохраненные на Сервере администрирования события);
- конфигурационную информацию о структуре групп администрирования и клиентских устройствах;
- хранилище дистрибутивов программ для удаленной установки (содержимое папок Packages, Uninstall, Updates);
- сертификат Сервера администрирования.

Ролевая группа

Группа пользователей мобильных устройств Exchange ActiveSync, которые обладают одинаковыми административными правами.

Ручная установка

Установка программы безопасности на устройство сети организации из дистрибутива программы безопасности. Ручная установка требует непосредственного участия администратора или другого IT-специалиста. Обычно ручная установка применяется, если удаленная установка завершилась с ошибкой.

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского". Сервер администрирования может также управлять этими программами.

Серверы обновлений "Лаборатории Касперского"

HTTP-серверы и HTTPS-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

Сертификат Сервера администрирования

Сертификат, который Сервер администрирования использует для следующих целей:

- аутентификации Сервера администрирования при подключении к Kaspersky Security Center 14 Web Console;
- безопасное взаимодействие Сервера администрирования с Агентами администрирования на управляемых устройствах;
- аутентификации Серверов администрирования при подключении главного Сервера администрирования к подчиненному Серверу администрирования.

Сертификат создается автоматически при установке Сервера администрирования и затем хранится на Сервере администрирования.

Состояние защиты

Текущее состояние защиты, характеризующее степень защищенности компьютера.

Состояние защиты сети

Текущее состояние защиты, характеризующее степень защищенности устройств сети организации. Состояние защиты сети включает такие факторы, как наличие на устройствах сети установленных программ безопасности, использование лицензионных ключей, количество и виды обнаруженных угроз.

Срок действия лицензии

Период, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Объем доступных функций и дополнительных услуг зависит от типа лицензии.

Точка распространения

Устройство с установленным Агентом администрирования, которое используется для распространения обновлений, удаленной установки программ, получения информации об устройствах в составе группы администрирования и/или широковещательного домена. Точки распространения предназначены для уменьшения нагрузки на Сервер администрирования при распространении обновлений и для оптимизации трафика в сети. Точки распространения могут быть назначены автоматически Сервером администрирования или вручную администратором. Точка распространения ранее называлась агентом обновлений.

Удаленная установка

Установка программ "Лаборатории Касперского" при помощи инструментов, предоставляемых программой Kaspersky Security Center Linux.

Управляемые устройства

Устройства сети организации, включенные в одну из групп администрирования.

Уровень важности события

Характеристика события, зафиксированного в работе программы "Лаборатории Касперского". Существуют следующие уровни важности:

- Критическое событие.
- Отказ функционирования.
- Предупреждение.
- Информационное сообщение.

События одного и того же типа могут иметь различные уровни важности, в зависимости от ситуации, при которой событие произошло.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии.

Хранилище резервных копий

Специальная папка для сохранения копий данных Сервера администрирования, создаваемых при помощи утилиты резервного копирования.

Хранилище событий

Часть базы данных Сервера администрирования, предназначенная для хранения информации о событиях, которые возникают в Kaspersky Security Center Linux.

Централизованное управление программой

Удаленное управление программой при помощи служб администрирования, предоставляемых Kaspersky Security Center.

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).

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.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

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 являются зарегистрированными товарными знаками или товарными знаками Cloud Software Group, Inc. и/или дочерних компаний в США и/или других странах.

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 являются товарными знаками Intel Corporation или ее дочерних компаний.

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.

UNIX – товарный знак, зарегистрированный в США и других странах, использование лицензировано X/Open Company Limited.

Zabbix – зарегистрированный товарный знак Zabbix SIA.